Network Time Server

NTS–200–GPS

User's Manual

NTS-200
Revision B
July 27, 2001

The information in this manual is subject to change without notice and should not be construed as a commitment by TrueTime, Inc. Furthermore, TrueTime, Inc. reserves the right, without notice, to make changes to equipment design as advances in engineering and manufacturing methods warrant.

The material described in this manual may be used or copied only in accordance with the terms of the license pertaining to the software and hardware referred to herein.

© 2001 TrueTime, Inc.
All rights reserved.
Printed in the U.S.A.

The following are registered trademarks or trademarks of their relative companies or organizations: Microsoft, Microsoft Windows, HyperTerminal, and Procomm.

The following are registered trademarks or trademarks of their relative companies or organizations: TrueTime, TrueTime, Inc.,Microsoft, Microsoft Windows, HyperTerminal, and Procomm. MD5 is the trademark or registered trademark of RSA Security, Inc.

This product includes software derived from the RSA Security, Inc. MD5 Message-Digest Algorithm, which is provided under license from RSA Security, Inc.

Network Time Protocol (NTP) ©David L. Mills 1992-2000.

Permission to use, copy, modify, and distribute NTP software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

Settings of NTS-200 Ethernet Ports

Record NTS-200 network configuration for the NET port below, for quick reference.

NET Port Ethernet Address:_____

NET Port IP Address:_____

NET Port Subnet Mask:_____

NET Port Default Gateway:_____

TRUETIME

3750 Westwind Boulevard
Santa Rosa, California 95403

t 707.528.1230
f 707.527.6640
w www.truetime.com

FCC Notice and Compliance Statement

Model: **Fiber Optic Modules, 150-702-1**
Fiber Optic Modules, 150-704-1
XL-AK GPS Receiver, 600-000
XL-AK GPS Receiver, 600-100
XL-AK GPS Receiver, 600-101
Network Time Server, NTS-200
Antenna Down\Up Converter, 142-6150

FCC Notice

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the computer and receiver.
- Connect the computer into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

FCC Compliance Statement

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE

DECLARATION OF CONFORMITY

In accordance with ISO/IEC GUIDE 22 and EN 45014

TrueTime, Inc.
2835 Duke Court
Santa Rosa, CA 95407 USA

Declares that the

NETWORK TIME SERVER
Model NTS-200

CONFORMS TO THE FOLLOWING EUROPEAN DIRECTIVES:

Low Voltage Directive 73 / 23 / EEC
Low Voltage Directive Amendment 93 / 68 / EEC
EMC Directive 89 / 336 / EEC

Safety:	**IEC 950:1991 + A1:1992 + A2:1993 + A3:1995 + A4:1997** **EN 60950 (1997) A1, A2, A3, A4**
EMC:	**EN 50082-1 (1997)** **EN 55022 Class B (1995)**

Issued: **April 24, 2000 at TrueTime, Inc., Santa Rosa, CA, USA**

I declare that the equipment specified above conforms to the above Directives and Standards.

4/24/00 — Manuf Engineering Manager

Date — Name — Title — Signature

European Representative: _____
Company Name and Location

_____

Date — Name — Title — Signature

Please fax or mail this survey back to TrueTime's Technical Documentation Department.
Fax: 707-527-6640
Mail: TrueTime
3750 Westwind Blvd.
Santa Rosa, CA 95403

User's Manual

Documentation Survey

Our Questions	**Your Answers**
Check off the main reasons you consult a manual.	General information How to do certain things Review, when needed Emergencies Other (please list)
When consulting the manual, can you find the information you need? (circle the number that fits)	not easily very easily 1 2 3 4 5 6
Can you find the information you need quickly? (circle the number that fits)	hard to find quick and easy to find 1 2 3 4 5 6
Please list any topics that were hard to find.	
Please list any topics that you couldn't find at all.	
How clearly is the manual organized? (circle the number that fits)	not clearly very clearly 1 2 3 4 5 6
Is the manual a useful size for you? (circle the number that fits.)	much too large just right 1 2 3 4 5 6
Is the font easy to read?	Big enough? Yes ❒ No ❒ Easy on the eyes? Yes ❒ No ❒
Would you like more educational information included about time and frequency in general?	Yes ❒ No ❒
If TrueTime published a thin, very basic, "how to" manual *without* all the detail and technical information in the current manual, would you have any use for such a publication?	I'd prefer it. ❒ I'd use them both. ❒ I probably wouldn't use it. ❒
Do you have use for an electronic (PDF) version of this manual?	Yes ❒ No ❒ If YES (and if you do not already have one), give us your email address and we will email you a PDF copy.

On a scale of 1- 6, please rate the following sections of the User's Manual for:

- clarity
- completeness
- usefulness

Circle the number of your rating: 1-2 = Unacceptable; 3-4 = Meets Expectations;
5 = Exceeds Expectations; 6 = Outstanding

	Unacceptable		**Meets Expectations**	**Exceeds Expectations**	**Outstanding**
General Information (including Specs)	1	2	3	4	5	6
Installation (cabling)	1	2	3	4	5	6
Quick Start Guide	1	2	3	4	5	6
Web/Telnet Access	1	2	3	4	5	6
Keypad Functions	1	2	3	4	5	6
Serial I/O Functions	1	2	3	4	5	6
Error (and other) Messages	1	2	3	4	5	6
Appendix A (NTP)	1	2	3	4	5	6
Appendix B (MD5)	1	2	3	4	5	6
Appendix C (Time/Daytime Protocols)	1	2	3	4	5	6
Appendix D (SNMP)	1	2	3	4	5	6
Table of Contents	1	2	3	4	5	6
Index	1	2	3	4	5	6

Please also write down any other suggestions for improving this manual:

Contents

1 General Information

Conventions 1-1
Overview of the NTS 1-2
Limited Warranty 1-2
Limitation Of Liability 1-2
Proprietary Notice 1-3
Physical Specifications 1-3
Environmental Specifications 1-4
Power Input Specifications 1-5
Certifications 1-5
Internal Timing Performance Specifications 1-5
Network Time Protocol Synchronization Specifications 1-6
Front Panel Interface 1-7
Interface Specifications 1-8
- NET Port Ethernet Interface 1-8
- Utility RS-232 I/O Interface 1-8

2 Installation and Start-Up

Site Preparation 2-1
- Mounting Instructions 2-1
- Necessary Equipment 2-2
- Antenna Information 2-3
- Antenna Location and Installation 2-3

Cabling 2-4
Power-Up 2-6
- Satellite Acquisition 2-6

Front Panel Interface 2-8
- Alphanumeric Display 2-8
- Keypad Operation 2-9

NET Port Network Parameters: First Time Configuration 2-13
Verify Functionality 2-14
Wrap-Up & Advanced Operation 2-14

3 Remote Operation

Web Access 3-1
Starting the Web Browser 3-1
Accessing the NTS Web Pages 3-2
Home Page 3-2
Time Information, GPS Status, and Network Information Pages 3-2
Configuration Control Login Page 3-3
Time Control, GPS Control, and Satellite Control Pages 3-3
Network Control Page 3-3
Leaving the Control Pages 3-7
Leaving the Web Interface 3-7
Telnet Access 3-7
Starting Telnet and Making a Connection 3-7
Ending Telnet 3-9
Serial Access 3-9
Serial Line Settings 3-9
HyperTerminal 3-10
Session Timers 3-15
Utility Port Session Timer 3-15
Telnet Session Timer 3-15
Web Control Session Timer 3-15

4 Serial or Telnet I/O Functions

Overview and Format 4-1
Command List 4-3
Function Commands 4-6
F03 – Time and Date Request 4-6
F18 – Software Version Request 4-6
F36 – NET Port Network Configuration Entry/Request 4-7
F53 – Operating Mode Request 4-7
F60 – Satellite List Request 4-8
F67 – Leap Second Information 4-10
F72 – Fault Status Request 4-10
Extended Function Commands 4-11
F100 BASET – 100 BASE-T/10 BASE-T Control 4-12
F100 DHCP – DHCP Control 4-13
F100 EA – Ethernet Address 4-14

F100 IP – IP Address 4-14
F100 SM – Subnet Mask 4-15
F100 G – Gateway 4-15
F100 IC – NET Port Network Configuration Entry/Request 4-16
F100 P – Change User Password 4-16
F100 ST – Self Test Status 4-17
F100 VER – Software Version Request 4-18
F100 CONFIG – FTP Configuration of NTP & SNMP Parameters 4-19
F100 LOCK – Remote Lockout 4-26
F100 L – Lock Display Request 4-26
F100 J - Jumper 4-27
F100 BH - Burn Host 4-27
F100 BU - Burn 4-28
F100 BUB - Burn BootLoader 4-29
F100 BF - Burn File System 4-29
F100 K I L L - Reboot 4-30
F100 BL - Burn Host Lock Request 4-31
F100 BLS - Burn Host Lock Set 4-31
F100 BLR - Burn Host Lock Reset 4-31
F100 PRESETALL - Password Reset All 4-32
F100 PN - Password System User Name Change 4-32
F100 PR - Password Reset 4-33
F100 PL - Password Lock Request 4-33
F100 PLS - Password Lock Set 4-34
F100 PLR - Password Lock Reset 4-34
F100 PE LIST - Peer List Request 4-34
F100 PE ADD - Peer Add 4-35
F100 PE REM - Peer Remove 4-35
F100 PI - PING 4-35
F100 PT - Time 4-35
Login/Logout 4-36
Operator Login 4-36
Guest Login 4-36
Logout 4-36

5 *NTS-Generated Messages*

Error Messages 5-1
LED System Status Alerts 5-3

Solid Red/Solid Orange 5-3
Informational Messages 5-3

A Network Time Protocol (NTP) V 3.0 Data Formats

NTP V 3.0 Data Format per RFC-1305 . . . . . A-2
NTP Data Packet A-2
SNTP V 3.0 Data Format per RFC-2030 . . . . . A-5

B MD5 Authentication and NTP Broadcast Mode

Introduction to MD5 Authentication Protocol B-1
NTP Broadcast Mode with MD5 Authentication B-3
NTP Broadcast Mode without Authentication B-4
Configuration of NTP on the Timeserver B-4
Configuration of NTP on the Time Client B-5

C TIME and DAYTIME Protocols

TIME Protocol as per RFC-868 . . . . . C-1
The Time Protocol Format C-1
DAYTIME Protocol as per RFC-867 . . . . . C-2
TCP Based Daytime Service C-2
UDP Based Daytime Service C-2
DAYTIME String Format C-2

D SNMP – Simple Network Management Protocol

About SNMP D-1
TrueTime SNMP Configuration D-2
Serial or Telnet Configuration D-4
TrueTime SNMP Enterprise MIB D-4

E Non-Standard Features

Index

1

General Information

This manual provides you with all of the information necessary to properly install and operate the NTS-200 Network Time Server (hereafter referred to as the NTS). Optimization for time functionality means that accurate position readouts are not available. The information in this manual includes any normal maintenance and adjustment data that may be required to facilitate field repairs.

1.1 Conventions

The conventions used in this manual are:

Text	=	Indicates body text.
Italics	=	Emphasizes important information.
	=	Used with bold text to call attention to important information.
<Key>	=	For input, refering to keys that are labeled on your keyboard. For example, <**Enter**> means press the Enter key for a line terminator; <**SP**> means press the spacebar to enter a space.
KEYPAD PUSH BUTTONS	=	Used to indicate push-buttons on the unit: Press *SAVE*.
Bold	=	Used to show messages, prompts, menus, items in selection lists, etc., that appear on a computer screen and require action on your part. For example, Press the **Submit Changes** button.
`text`	=	Used to display output character strings.
`text`	=	Used to indicate text you should enter with your keyboard, *exactly* as printed.

1.2 Overview of the NTS

The NTS is a high-performance Network Time Protocol (NTP) server that reports time with extreme accuracy, using the Global Positioning System (GPS) as a synchronization source. The NTS provides Internet Protocol (IP) network time synchronization over Ethernet connected networks via NTP, developed by Dr. David Mills at the University of Delaware. The NTS currently supports versions 2 and higher of the NTP, RFC-1305, as well as the Simple Network Time Protocol (SNTP), RFC-2030. In addition, the NTS responds to TIME protocol requests, RFC-868. For details about these protocols, refer to Appendix A and Appendix B in this manual.

The main feature of the NTS web interface is its ability to perform setup and control operations from a remote location, using the Internet or TCP/IP LAN (see Chapter 3). The protocol used is either Telnet or HTTP. An NTS has an RJ-45 Ethernet connector on its NET Port, providing NTP and IP access, and a 9-pin D serial connector for serial input/output.

1.3 Limited Warranty

Each new product manufactured by TrueTime is warranted for defects in material or workmanship for a period of one year from date of shipment (“Limited Warranty”). Defects in material or workmanship found within that period will be replaced or repaired, at TrueTime's option, without charge for material or labor, provided the customer returns the equipment, freight prepaid, to the TrueTime factory under this limited warranty. TrueTime will return the repaired equipment, freight prepaid, to the customer's facility. This one year Limited Warranty does not apply to any software or to any product not manufactured by TrueTime.

1.4 Limitation Of Liability

By purchasing any product from TrueTime, the Buyer consents to and agrees that the Buyer's sole and exclusive remedy for any damages or losses incurred by the Buyer, as a result of TrueTime's breach of its one-year Limited Warranty for defects in materials and workmanship or otherwise in connection with any claim respecting the product, shall be limited to the repair or replacement of the product or a refund of the sales price of the product.

In no event shall the Buyer be entitled to recover consequential damages or any other damages of any kind or description whatsoever.

1.5 Proprietary Notice

THIS DOCUMENT, WHETHER PATENTABLE OR NON-PATENTABLE SUBJECT MATTER, EMBODIES PROPRIETARY AND CONFIDENTIAL INFORMATION AND IS THE EXCLUSIVE PROPERTY OF TRUETIME, INC. IT MAY NOT BE REPRODUCED, USED OR DISCLOSED TO OTHERS FOR ANY PURPOSE EXCEPT THAT FOR WHICH IT IS PURCHASED OR LOANED.

1.6 Physical Specifications

The NTS fits in a standard 1U (1.75-inch [4.445-cm]) high, 19-inch (48.26-cm) rack mount package (see page 2-1 for mounting instructions) and has the following physical specifications:

NTS Chassis, with rails and handles	
Size:	1.73 in x 17.00 in x 11.63 in (4.39 cm x 43.18 cm x 29.54 cm)
Weight:	4.21 lb max. (1.91 kg)
Standard Antenna	
Size:	2.625 in dia. x 1.5 in (6.67 cm dia. x 3.81 cm)
Weight:	0.55 lb (0.250 kg) (including mounting mast)
Power Regulated:	+12 V @ <25 mA
Frequency (L1):	1575.42 MHz Coarse Acquisition (C/A) Code
Optional Down/Up Converter	
If you have this option, please refer to the manual for: TrueTime Model 142-6150, Antenna Down/Up Converter	
Antenna Cable (for Standard Antenna)	
Type:	RG-59 Attenuation at 1575.42 MHz should be no more than 10.5 dB per 100 feet (Belden 9104 or equivalent)
Length:	50 ft (15.24 m) [available in lengths up to 200 ft (60.96 m)]
Weight:	1.2 lb (0.545 kg)
Antenna Cable (for optional Down/Up Converter Antenna)	
If you have this option, please refer to the manual for: TrueTime Model 142-6150, Antenna Down/Up Converter	

The NTS-200 requires a 12 V antenna and may severely damage any antenna that does not support 12 V. For non-standard antenna types, contact TrueTime for assistance.

1.7 Environmental Specifications

The environmental specifications of the NTS are:

Operating Temperature	
NTS Module:	0 to +50 °C (+32 to +122 °F)
Antenna:	–40 to +70 °C (–40 to +158° F)
Maximum Rate of Change:	8 °C per hour
Storage Temperature	
NTS Module:	–50 to +85 °C (–40 to +185 °F)
Antenna:	–55 to +85 °C (–67 to +185 °F)
Maximum Rate of Change:	15 °C per hour
Operating Humidity	
NTS Module:	0% up to 95%, non-condensing
Antenna:	100%, condensing
Storage Humidity	
NTS Module:	0% up to 95%, non-condensing
Antenna:	100%, condensing
Operating Altitude	
NTS Module:	Maximum 4 km
Storage Altitude	
NTS Module:	Maximum 12 km
Shock & Vibration Requirements	
In Shipping Container:	Per ISTA Procedure 2A
Bench Handling without Shipping Container:	Per EN60068-2-31

1.8 Power Input Specifications

The power input specifications of the NTS are:

Power Input	
AC Mains: (base model)	100 to 240 VAC, 47–440 Hz IEC 320 Connector
–48 VDC (optional):	–36 to –60 VDC 4 position Barrier Strip Connection Fuse: 1A Slow-Blow (rear panel)
Power Requirement:	<20 W maximum

1.9 Certifications

FCC

CE (applies to base model only)

UL (applies to base model only)

1.10 Internal Timing Performance Specifications

The absolute time and frequency characteristics of the NTS are essentially those of the input synchronization source. The relative synchronization characteristics given here reflect the capabilities of the NTS to preserve the time and frequency characteristics of its synchronization source.

The NTS output signal timing and frequency specification, relative to input synchronization source, is:

Internal Timing Accuracy: <5 μs to UTC when synchronized via GPS

During a synchronization input outage, following initial synchronization of the NTS to the input synchronization source, the time maintained in the unit diverge from the input at the rate of approximately 6 parts in 10^{-6}, if the ambient temperature is maintained within ± 3 °C.

1.11 Network Time Protocol Synchronization Specifications

The NTS hardware is designed specifically to implement the NTP server function. As such it was carefully designed to operate with the TrueTime real time operating system to minimize the unknown latencies in timestamping the received and transmitted NTP packets. The NTP Packet timestamp accuracy specifications are:

Received Timestamp Accuracy: <0.1 ms, relative to synchronization source

Transmitted Timestamp Accuracy: <0.1 ms, relative to synchronization source

Network timing accuracy is limited to 1-10 ms typical.

At these levels of accuracy, the realizable NTP synchronization accuracy of any host is determined by the repeatability of the network and client delays, *not* by the NTS timestamp uncertainty.

The NTS supports the following protocols:

- Telnet RFC-854
- DAYTIME RFC-867
  available in both TCP and UDP protocols
- TIME RFC-868
  available in both TCP and UDP protocol
- FTP RFC-959
- SMI RFC-1155
- SNMP RFC-1157
- MIB. RFC-1212
- MIB II RFC-1213
- NTP ver. 4.0 . . . . . .N/A
  (backwards compatible with NTP v.2, RFC-1119, and v.3, RFC-1305**)
- MD5 . . . . . .RFC-1321
- SNTP RFC-2030
- HTTP . . . . . .RFC-2068 and 2616
- DHCP RFC-2132

* SMI = Structure of Management Information

** The NTS does not implement the “authenticator field” of the NTP packet as described in Appendix C of RFC-1305.

Complete RFC information is available at the following web site: http://www.ietf.org/

An NTP or SNTP client, compatible with the computer platform you use and configured to use the NTS NET Port IP address, is required for accurate network synchronization. In this manual, refer to Appendix A and Appendix B for details about NTP and SNTP protocols, and Appendix D for details about SNMP and MIB.

1.12 Front Panel Interface

This section provides a general description of the NTS front panel input devices. For details about how to enter commands and interpret display readouts, see "Overview and Format" on page 4-1.

The NTS front panel is your primary interface with the system. Input is through six keypad buttons (four directional, *SET-UP* and *SAVE*). Output is through the two-line, 20-character alphanumeric display (see Figure 1-1, below).

Two front panel mounted, tri-color LEDs reflect the status of the NTS. The system status indicator at the left end of the front panel has five different displays:

If the System Status Displays...	It Means...
Solid Red	No signal from time source, or major alarm fault detected
Solid Orange	The NTS is synchronized to Network Time Servers through NTP
Blinking Green	The NTS is fully operational

Possible causes and solutions for problems resulting in a solid red or solid orange display are discussed in "LED System Status Alerts" on page 5-3.

The connection active indicator, labeled "ACT" and located to the right of the NET Port's RJ-45 plug, indicates the connection speed on the NET Port:

"ACT" Display	Network Connection Speed
Solid Yellow	10Base-T
Solid Green	Up to 100Base-T

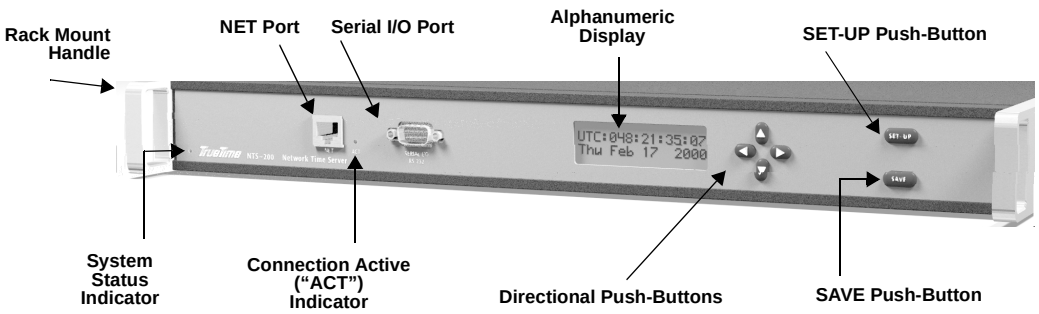


Figure 1-1 NTS Front Panel

2

Installation and Start-Up

2.1 Site Preparation

2.1.1 Mounting Instructions

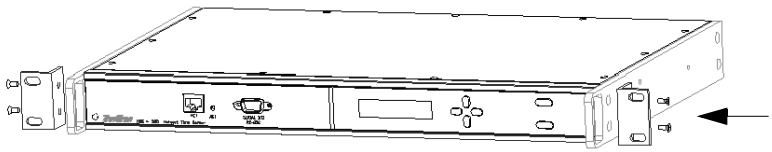
To securely mount the NTS-200 in any EIA standard 19-inch (48.26-cm) rack system, use the equipment supplied in TrueTime's Rack Mount Kit and follow the steps outlined below.

The Rack Mount Kit contains:

- 2 mounting brackets (part number 206-719)
- 4 flat-head, Phillips screws (part number 241-008-005, 8-32 x 5/8)

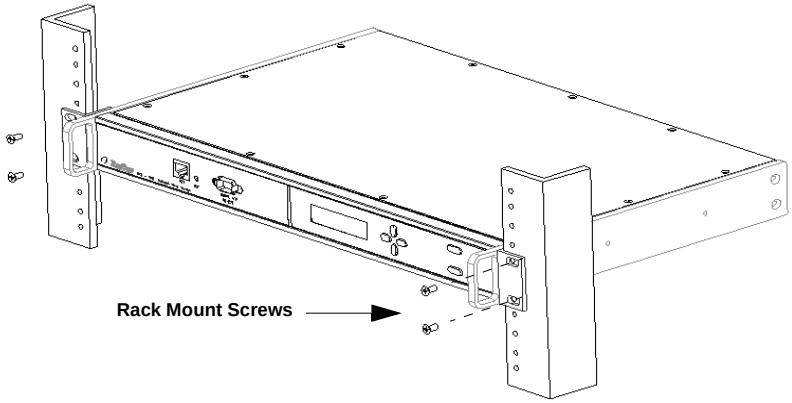
To rack mount the NTS-200:

1. Remove and discard the two factory-installed flat head (Phillips) screws from the front end of an NTS-200 side panel.
2. Place a rack mount bracket on the side panel, so that the countersunk screw holes in the bracket line up with the screw holes in the panel.



3. Place two of the screws from the Rack Mount Kit through the holes in the bracket and into the NTS-200.
4. Tighten the screws to the following specifications:
   Use a #2 size Phillips bit with an inch ounce torque setting of 4 ¼ to 4 ¾ (high).
5. Repeat steps 1-4 to install the other rack mount bracket on the unit's other side panel.

6. Place the NTS-200 in a 1 ¾ inch (4.445 cm) opening in any EIA Standard 19 inch (48.26 cm) rack system, and position the unit so that the rack holes line up with the holes in the bracket.



7. Use the appropriate screws to secure the brackets to the rack.
8. Ensure that the operating ambient temperature does not exceed +50 °C.

Installation requires the use of standard rack mount hardware.

2.1.2 Necessary Equipment

The equipment you need to get started includes:

- Power source
- GPS antenna connection that supports 12 V
- An Ethernet LAN with one port available for the NTS network connection
- An Ethernet cable with an RJ-45 connector for the NET Port (Category 5 Ethernet cable is recommended for 100Base-T operation)
- A set of network address parameters for the NET Port that delivers NTP time and allows remote control of the unit over the Internet

The NTS-200 requires a 12 V antenna and may severely damage any antenna that does not support 12 V. For non-standard antenna types, contact TrueTime for assistance.

Optionally, you can add an RS-232 serial interface for local control using a terminal emulation program. This requires:

- A serial interface device, either PC or dumb terminal capable of 9600 8N1
- An RS-232 cable, and null modem connector, to connect the 9-pin D RS-232 port to the serial device

The NTS is capable of basic operation without an RS-232 connection, and retains all configuration data in memory.

2.1.3 Antenna Information

Voltage Requirement and Signal Levels

The NTS requires a 12 V antenna. Any antenna that does not support 12 V may be severely damaged if plugged into the NTS.

The GPS Synchronized Receiver, integral to the NTS, operates on the L1 (1575.42 MHz) signal and the C/A code (1.023 MHz bit rate) with a minimum signal level of –162.0 dBW and a maximum signal level of –137.0 dBW. The antenna system supplied is designed to provide the proper signal levels to the receiver with the cable length supplied.

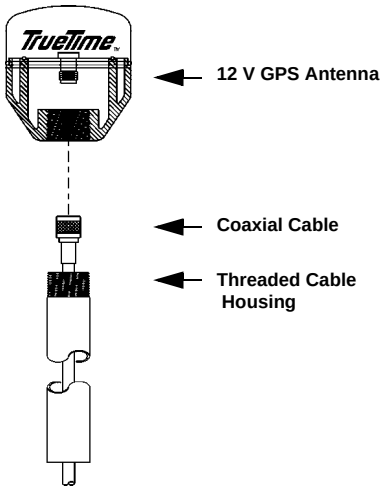


Figure 2-1 Basic Antenna Components

Use of a Splitter

To run multiple units with a single 12 V antenna, use a splitter. Do *not* use a BNC "T" connector.

Lead-In Cable

The L1 GPS antenna is designed to operate with up to 200 ft (60.96 m) of RG-59 coax cable. The optional Down Converter is designed to operate with up to 1,500 ft (457.2 m) of RG-58 coaxial cable. For details and illustrations on cabling, see page 2-4.

2.1.4 Antenna Location and Installation

When selecting a site for the antenna, find an outdoor location that provides full 360-degree visibility of the horizon. In most cases, this means locating the antenna as high as possible. Any obstruction will degrade unit performance by blocking the satellite signal or causing a reflection that cancels some of the signal. Blocked signals can *significantly* increase the time for satellite acquisition, or prevent acquisition all together.

Mast Mounting

Mast top mounting is the preferred mounting method and special brackets are provided to mount the antenna to a pipe or the peak of a building. The antenna mounting mast should be 2-inch (5.08-cm) water pipe or conduit. The mast must be rigid and able to withstand high winds without flexing. Guy wires may be used to stabilize a mast longer than 10 ft (3.048 m)

Multipath cancellation is caused by reflected signals that arrive at the antenna out of phase with the direct signal. Reflective interference is most pronounced at low elevation angles from 10 to 20 degrees above the horizon. You may extend mast height to prevent multipath cancellation. The antenna should be at least 3.28 ft (1.0 m) from a reflecting surface. The figure at the right shows the recommended mounting of the antenna to the mast.

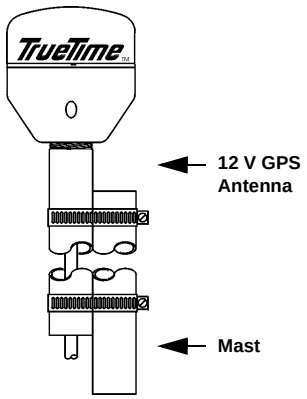


Figure 2-2: Mast Mounting Illustration

2.2 Cabling

Refer to the figures below for NTS connector locations. The numbers in the drawing refer to that connector's position in Table 2-1.

Connect the cables in the order listed in Table 2-1 below. In order to avoid network addressing conflicts, be sure to configure network parameters *before* connecting the Ethernet cable.

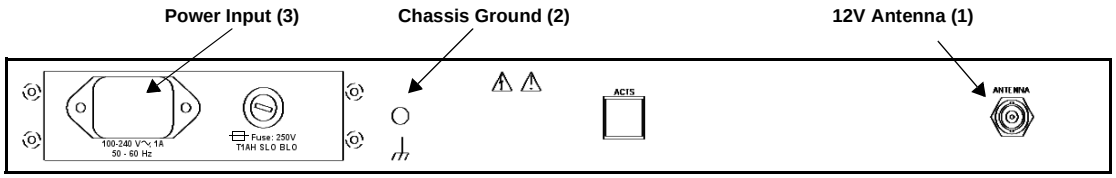


Figure 2-3: NTS Back Panel Cabling Illustration (AC Mains)

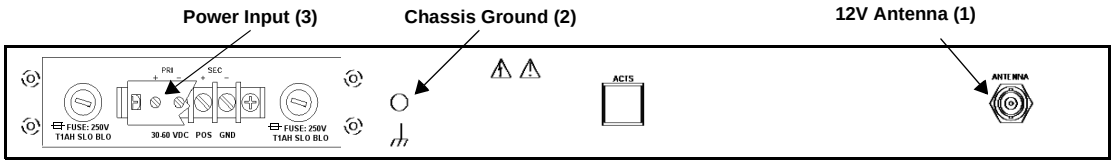


Figure 2-4: NTS Back Panel Cabling Illustration (–48 VDC)

For the –48 VDC model, connect the rear panel chassis ground to your system ground, the positive connection from the power supply to the "+" of the rear panel terminal strip, and the negative connection from the power supply to the "–" of the rear panel terminal strip.

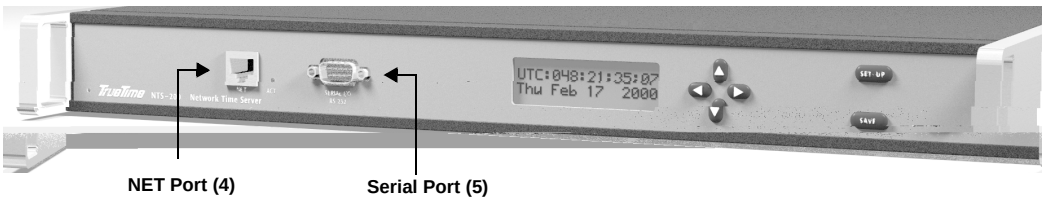


Figure 2-5: NTS Front Panel Cabling Illustration

2.3 Power-Up

At power-up (cold boot), the front-panel display is blank.

After about 10-12 seconds, the display reads:

```
NTS-200
Booting...
```

After another 10 seconds, the display reads:

```
NTS-200
Loading...
```

System software initialization takes about 18 seconds, after which the display reads:

```
Software
Load Successful
```

Display initialization takes another 12 seconds, after which the NTS starts searching for satellites. The display reads:

```
Searching for
Satellites
```

You can now enter data to the NTS through the front panel keypad or serial/Telnet interface. Data entry requires completion of display initialization.

Satellite acquisition may take up to 20 minutes. Display messages indicate the sequence, such as:

```
Satellites
Tracked =  1
```

2.3.1 Satellite Acquisition

Satellite acquisition begins at power-up and continues until power-down. Time to first satellite acquisition depends on many factors. The following paragraphs describe some of the possible events that affect satellite acquisition times.

The NTS attempts to acquire satellites, not knowing which satellites are visible. The search continues until a satellite is acquired. After first satellite acquisition, time is acquired from the satellite and the receiver returns to normal operation. This procedure may take from as little as 3 minutes to as long as 20 minutes, depending upon current satellite visibility.

If the current position is unknown or in error by more than 1 km (0.62 miles), acquisition typically requires from 3 to 20 additional minutes to locate current antenna position, reacquire satellite almanac and ephemeris data, and deliver UTC time. However, since the NTS is optimized for time functionality, accurate position readouts are not available.

NTP stabilization, which allows the unit to display accurate time and which may take 8-10 minutes, begins after the NTS acquires the 4th satellite. During this procedure, the display alternates between an "Initializing" message and notification of which satellites have been newly acquired. NTP stabilization usually takes place between acquisition of the 5th and 6th satellites.

During NTP stabilization, the display reads:

```
Initializing
NTP...
```

```
Satellites
Tracked =  X
```

where:

X = the number of the next satellite the NTS acquires.

Once stabilized, NTP displays UTC time and the current date on the front panel display in the following default format:

```
UTC: DDD;HH:MM:SS
ddd<SP>mmm<SP>nn<SP>yyyy...
```

where:

DDD	=	day of year
HH	=	hour
MM	=	minutes
SS	=	seconds
ddd	=	day of the week (abbreviations are: "Sun", "Mon", "Tue", "Wed", "Thurs", "Fri", "Sat"
mmm	=	month (abbreviations are: "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec")
nn	=	day of month
yyyy	=	year

An illustration of the front panel default display appears on the next page.

Once the NTS has synchronized itself, then it is ready to respond to time requests that it receives over the network through supported protocols. During interruptions of the synchronization input, the NTS estimates the quality of the time it is able to provide to clients and updates the fields of the NTP packet appropriately.

If the NTS has saved a good current average position and has saved recent UTC leap second information, it typically locks to GPS in 3 to 5 minutes and delivers UTC time.

2.4 Front Panel Interface

Figure 2-6 Front Panel Display and Keypad

The NTS front panel provides input through 6 keypad push-buttons (four directional keys, *SET-UP*, and *SAVE*), and output through the two-line, 32-character alphanumeric LCD.

Use the keypad for initial system configuration (see page 2-13).

2.4.1 Alphanumeric Display

The two-line, 32-character alphanumeric display has several functions:

Table 2-2 Alphanumeric Display Functions

The Display Shows	During	How to Access
Status Messages	Start-Up and Initialization	Default
Satellite Acquisition Status	Start-Up and Initialization	Default
Current UTC Date and Time (in real time, as illustrated above)	Normal Operation	Default* *If another display is active during normal operation, press *SET-UP* repeatedly until the UTC display appears
Ethernet Address Parameters, starting with IP Address	Normal Operation	Press the *SET-UP* push-button
Remote Control Status	Normal Operation	Press the *SET-UP* push-button after viewing the Default Gateway display

Front Panel Network Parameter Display

The following sequence appears on the front panel alphanumeric display when you repeatedly press the *SET-UP* push-button. After first power-up, if you enable the Display Security feature, you must enter your user ID and password before these parameters appear on the display.

The values illustrated below are examples only. If you are ready to configure the NTS-200 for the first time, go now to Section 2.5 "NET Port Network Parameters: First Time Configuration" on page 2-11.

1. IP Address.
   An example of the display is:

   ```
   255.054.000.034
   IP ADDRESS
   ```

2. Subnet Mask.
   An example of the display is:

   ```
   255.054.000.034
   SUBNET MASK
   ```

3. Default Gateway.
   An example of the display is:

   ```
   255.054.000.034
   DEFAULT GATEWAY
   ```

4. DHCP.
   An example of the display is:

   ```
   DHCP Status
   OFF
   ```

5. Remote Control.
   An example of the display is:

   ```
   Remote Control
   Unlocked
   ```

6. Display Security.
   An example of the display is:

   ```
   Display Security
   Off
   ```

7. Display Security Logout.
   An example of the display is:

```
Display Security
Logout
```

Whenever you save changes to any network parameter in this sequence, the NTS-200 automatically reboots (this does not include the DHCP, Remote Control, and Display Security functions).

The Remote Control feature determines the availability of remote access to the NTS-200. The default setting is "Unlocked", which allows use of the Telnet or web interface for set-up and control operations (see Chapter 3 for how to set up Telnet, and Chapter 4 for how to issue F-series function commands). You can lock the NTS-200 from a remote location using the F100 LOCK command, but after having done so, you can not remotely unlock it. You can *only* unlock the NTS-200 from the keypad. For more information, see "Keypad Entry Guidelines" above, and Section 4.4.12 "F100 LOCK - Remote Lockout" on page 4-25.

Entering the User ID and Password

You cannot change the ID and password via the keypad, only via F100 commands.

The Display Security feature prevents unauthorized users from setting or modifying NTS-200 parameters. When you first receive the unit, the security setting is off (factory default).

To view the current security setting, scroll through the parameter list using the *SET-UP* push-button until **Display Security** appears. To enable Display Security, press any directional push-button. The security setting changes from "OFF" to "ON". You can now enter your user ID and password, as per the procedure described below.

Once you enable the Display Security feature, it remains "ON" until you manually disable it.

Enter user IDs and passwords with the front panel directional push-buttons, as follows:

- Press the ↑ directional push-button to start at the letter "i" and move backwards through the alphabet, symbols and numbers.
- Press the ↓ directional push-button to start at the letter "r" and move forward through the alphabet, symbols and numbers.
- Press the ← or → directional push-buttons to reposition the cursor. During password entry, pressing the → directional push-button not only advances the cursor position, but also changes the previously entered character to a "*". If you make an incorrect entry, reposition the cursor and re-enter the character.

To enter the user ID and password, follow these steps:

1. Press the *SET-UP* push-button until **ID:/Password:** appears, with the cursor positioned on the **ID:** line (the *SET-UP* push-button toggles cursor position between the two lines).

2. Enter a character with either the ↑ or ↓ arrow, as described above.
3. Press the → directional push-button to advance the cursor.
4. Repeat step 2 and step 3 until you have entered all the user ID characters.
5. Press the *SET-UP* push-button to reposition the cursor on the **PW:** line.
6. Enter password characters using step 2 and step 3 above.
   Every time you press the → directional push-button, the previous character becomes a "*".
7. After entering the last password character, press the → arrow once more, so that all characters are "*"s.
8. Press the *SAVE* push-button to save all entries and enter the parameter display sequence.

If you followed this procedure correctly, the first parameter (IP Address) appears and you can now enter initial system parameters as per the procedure in Section 2.5 on page 2-11. If there was a problem with security set-up, a message appears: "Invalid Login ID or Password."

Once you have set the user ID and password, you must enter them whenever using the front panel alphanumeric display to review or modify system parameters. For a quick review, or to modify parameters remotely, use the NTS-200 web interface or a serial connection.

Further Precautions

After 10 minutes without any front panel push-button activity, the NTS-200 automatically times out the security feature. You must re-enter user ID and password to review or modify system parameters through the front panel alphanumeric display.

However, under circumstances when you must protect the NTS-200 *before* the 10-minute time out, you can do this manually with the Display Security Logout feature.

To manually logout of Display Security:

1. Press the *SET-UP* push-button to scroll through the parameter list until **Display Security Logout** appears.
2. Press the *SAVE* push-button.
   The default UTC time and date display appears.

After logging out, you must re-enter the user ID and password to review or modify system parameters through the front panel alphanumeric display.

Disabling Security

The Display Security feature remains "ON" until you manually disable it. To disable the Display Security feature:

1. Press the *SET-UP* push-button until **Display Security** appears.
2. Press any directional push-button to change the security setting from "ON" to "OFF".
3. Press the *SAVE* push-button.
   The default UTC time and date display appears, and system parameters can now be reviewed or modified by anyone.

2.5 NET Port Network Parameters: First Time Configuration

After connecting the GPS antenna, supplying power to the NTS, and achieving successful stabilization, stop cabling and configure the network parameters and functions for the first time. Then connect the Ethernet cable and, optionally, the serial cable. Observing this order of events ensures that the IP Address is correct and sets operating speed at 10Base-T.

To change the maximum operating speed to negotiate between 10/100Base-T on networks that support the higher speed, see Step 9 below.

The configurable NET Port network parameters and functions are:

- IP Address
- Subnet Mask
- Default Gateway
- DHCP
- Remote Control

For this first configuration, enter the appropriate parameter values and function settings through the front panel keypad. Optionally, you could use the serial port (referred to in this manual as the "Utility Port") through a serial device connected at **9600 8N1**. Subsequently, you can edit parameter values and function settings through the keypad, the web interface, the Utility Port, or using Telnet (see Section 4.4 "Extended Function Commands" on page 4-11).

To set the NET Port network parameter values and function settings for the first time:

1. Press the *SET-UP* push-button to display the IP Address.
2. Position the cursor under the digit you want to change using the ← and → buttons.
3. Increase or decrease the value with the ↑ or ↓ buttons.
4. Press the *SAVE* push-button to store the new values and proceed to the next screen. If you do not press *SAVE*, your entry will be lost.
5. Use Steps 2 – 4 above to set and store a new Subnet Mask value.
6. Use Steps 2 – 4 above to set and store a new Default Gateway value.
7. Review the current DHCP function setting, then use Steps 3 – 4 above to set and store a new DHCP setting, if appropriate (see the note below before changing this setting). The directional push-buttons toggle between setting options.
8. Review the current Remote Control function setting, then use Steps 3 – 4 above to set and store a new setting.
   The directional push-buttons toggle between setting options.
9. End the configuration sequence by pressing *SAVE*.
   The NTS automatically resets if you have saved any changes to any network parameter (excluding Remote Control), and sets the operating speed at 10Base-T.

2.6 Verify Functionality

To verify that the unit is running:

1. Ping the NET Port IP Address.
2. If this action fails, check the configuration values assigned to the NET Port. Correct parameters as necessary using the front panel keypad, described above, or the serial/Telnet Function F100 IC command, described on page 4-15.
3. If ping fails again, verify with your system administrator that the values used are correct. Then re-enter parameters as necessary.

2.7 Wrap-Up & Advanced Operation

When the LAN interfaces are operational and time is being reported, the unit has achieved its basic level of functionality. For “quick start” information, see the Quick Start card that came packaged with this manual. For remote operation, see Chapter 3. For details on serial/Telnet commands, see Chapter 4.

If you wish to configure NTP client mode, or to use SNMP (the NTS supports a SNMP version 1 agent with the MIB II and Enterprise MIB databases), you must first edit the ntp.conf and snmp.conf files (see Section 4.4.11 “F100 CONFIG – FTP Configuration of NTP & SNMP” on page 4-18 for details).

3

Remote Operation

TrueTime's NTS is an advanced network time server that provides accurate time over an Ethernet connection to multiple client sites. A great strength of the NTS is its remote control capability. You can configure parameters through command line input using Telnet from a distant terminal, or use the NTS web interface to program the unit over the Internet, from anywhere in the world.

You do not need a web connection for normal NTS operation.

The NTS reports time with extreme accuracy, using GPS as a synchronization source. Optimization for time functionality means that accurate position readouts are not available.

3.1 Web Access

The main feature of the NTS web interface is its ability to perform setup and control operations from a remote location, using the Internet or TCP/IP LAN. The protocol used is either Telnet or HTTP. Telnet is a standard Internet communications program that is bundled with Windows 95/98/NT and connects to the NTS through its NET Port. HTTP access is provided via any standard Web Browser (such as Microsoft's Internet Explorer or Netscape's Navigator/Communicator).

You can also disable remote control capability and secure the NTS from a remote location, (see "F100 LOCK – Remote Lockout" on page 4-26). However, once you have issued this command, you can only *unlock* the unit from the keypad.

3.1.1 Starting the Web Browser

To use the web interface, launch any Java-capable and frames-compatible web browser such as Microsoft Internet Explorer (IE version 3.0 or later, available at www.microsoft.com), Netscape Navigator (version 3.0 or later) or Netscape Communicator (any version; Netscape browsers are available at www.netscape.com).

3.1.2 Accessing the NTS Web Pages

In the **Location** field (Netscape), the **Address:** field (IE), or the equivalent field in the window of a different web browser, enter the IP address assigned to the NET Port of the NTS in the following format:

```
http://<ipaddress>
```

An example of an NTS NET Port IP address is: http://192.168.1.1

The available web pages are: **Home**, **Time Information**, **GPS Status** (which takes you to the **Satellite Status** page), **Network Information**, and **Configuration Control Login**. When entering from the IP address, your first stop is the **Home** Page.

3.1.3 Home Page

After entering the NET Port IP address, TrueTime's home page appears in the browser window. You can access all the other web pages from the home page, so for future quick access, you can bookmark it (in Netscape) or add it to your browser favorites (in IE).

3.1.4 Time Information, GPS Status, and Network Information Pages

From the **Home** page, click the **Time**, **GPS**, **Network,** or **Controls** buttons to display the **Time Information**, **GPS Status**, **Network Information**, and **Configuration Control Login** pages, respectively. You can navigate from page to page using the corresponding buttons at the top of the web browser window.

The values displayed on these pages are static, i.e.; they may not reflect changes that occurred following the initial display of the page. An example of this is **UTC Time** field on the **Time Information** page. The time shown is the time read at the instant the web page first displayed, and does not update with the most recent values until you click the **Reload** or **Refresh** button of your web browser.

To reach the **GPS Satellite Status** page, click the **GPS** button on the **Home** page or any status page, which takes you to the **GPS Status** page. From there, click the **Satellites** button.

3.1.5 Configuration Control Login Page

The **Configuration Control** page is your gateway to remote control of the NTS. After logging in here, you can use the buttons at the top of the page to navigate to the **Time Control**, **GPS Control**, **Satellite Control**, and **Network Control** pages (any changes you make on the **Network Control** page cause the NTS to reboot).

To reach the **Configuration Control Login** page, click the **Controls** button located at the top of the **Home** page or at the top of any of the status pages.

Enter the user name **`operator`** and the default password **`mercury`** in the corresponding fields on this page, then press <**Enter**> or click the **Press to Continue** button. The page refreshes. Look in the **Status Message Window** to see whether or not the login passed (you may have to scroll down to see it). If the **Status Message Window** shows that login failed, re-enter the user name and default password and click **Press to Continue** again.

Status Message Window

Regularly check the **Status Message Window**. If, for example, a processing error or transient network problem causes one or more of your entries to fail, a notification message appears here. If this happens, simply resubmit the entry. If you encounter repeated failures, use the Telnet or serial interface to make those entries.

As with all password protection, to ensure security, please change the default password as soon as possible using the "F100 P" command (see page 4-16). Password changes can only be made using the serial or Telnet interface.

3.1.6 Time Control, GPS Control, and Satellite Control Pages

The values displayed on the **Time Control**, **GPS Control**, and **Satellite Control** pages are static, i.e.; they may not reflect changes that occurred following the initial display of the page. An example of this is the **UTC Time** field on the **Time Control** page. The time shown is the time read at the instant the web page first displayed, and does not update with the most recent values until you click the **Reload** or **Refresh** button of your web browser.

3.1.7 Network Control Page

To edit parameters on the **Network Control** page, enter the new values or, given the option, chose the appropriate values from radio button selections. Then press <**Enter**> or click the **Submit Changes** button. If you have changed any network parameter (IP Address, Subnet Mask, Default Gateway, and/or DHCP), the NTS resets automatically.

After any reset, do not submit further parameter changes until the unit fully reinitializes, that is, until you see the correct time and date on the front panel display.

To edit NTP or SNMP parameters, click either the **NTP Configuration** button or the **SNMP Configuration** button to reach their respective remote control pages.

Remote NTP Configuration

Configuring NTP parameters involves editing the values in the "ntp.conf" and "ntp.keys" files. You can do this from the **Network Controls** page (for details on configuring NTP using serial/Telnet commands, see page 4-21). See Appendix B for a thorough discussion about the use of NTP, with and without MD5 authentication.

To configure NTP parameters over the Internet:

1. From the **Network Controls** web page, click the **NTP Configuration** button.
   The **Network Time Protocol Configuration** window appears.
2. Scroll through the "ntp.conf" file.
   The window contains the following default information:

```
Note= ALL servers are optional.  If your GPS antenna is connected
and positioned correctly, the servers listed here are not used.
These servers are used only when the GPS unit fails. GPS failure is
detected automatically.  Note that when the NTS is using these
timeservers the system is, at best, running with 20 millisecond
precision.  Up to 10 NTP servers can be assigned in this file.  The
addresses below are examples, and should be changed as required by
your network configuration.

The following are public TrueTime NTP Timeservers.  Uncomment one
or both to enable NTP fallback to TrueTime if GPS synchronization
is lost.  Add any other server address.

server     206.54.0.20
server     206.54.0.21

Private time servers (example only).

server     192.168.1.35

Uncomment the "broadcast" line below to enable NTP broadcast mode
with MD5 using key 1. The key may be omitted, but is less secure.
If a key is used here, a corresponding entry for that key must
appear in the NTP key file.  A maximum of 20 keys for broadcast can
be defined on this line.

broadcast     192.168.1.255     key 1

The line below lists the currently trusted keys. See the NTP keys
file for the actual keys and their corresponding key numbers. Keys
1 and 2 are listed as an example.  All keys listed must appear in
the NTP keys file.  Note= to ensure maximum security, remember to
change the keys on a regular basis.  A maximum of 20 trusted keys
can be defined on this line.

trustedkey     1     2
```

3. Edit the file.
4. Press <**Enter**> or click the **Submit Changes** button near the bottom of the page.
   The NTS resets, starting up with the new parameters in place.

5. Scroll down to the **MD5 Keys File:** window.
   The window contains the following default information:

```
Define your own keys and change them frequently.  These keys must
match key IDs and values assigned in your NTP client software
setup.  Note: to ensure maximum security, remember to change the
keys on a regular basis.  Key values are a
maximum of 32 characters.  A maximum of 24 keys may be
entered in this file.

Example keys follow.

Id    M    Value
----  ---  --------
1     M    truetime
2     M    xyz123
```

   where 1 and 2 are key identifiers (for maximum security, use a unique combination of 32 letters and numbers for each key identifier).

6. Edit the file.

7. Press <**Enter**> or click the **Submit Changes** button nea057 T.2ne thpa(e)- Tge).
   ThNTS a sess, s tt2arxi thn sea

Remote SNMP Configuration

By default, SNMP is disabled. To use it, or to configure any other SNMP parameters, involves editing the values in the `temp/` directory. The fastest and easiest way to do this is from the **Network Controls** page (for details on configuring SNMP using serial/Telnet commands, see page 4-24). See Appendix D for a thorough discussion about SNMP.

To configure SNMP parameters over the Internet:

1. From the **Network Control** page, click the **SNMP Configuration** button.
   The SNMP Configuration File window appears.

Scroll through the "snmp.conf" file.
The window contains the following default information, with each string appearing as a single line on your display:

```
MIB=/config/ttmib.o,
GenTraps=NO,
sysContact=TrueTime. 707-528-1230,
sysName=NTS-200,
sysLocation=Santa Rosa CA 95407,
NAME=pubic,VIND=1,TRAP=YES,ACCESS=R,IP=192.168.001.230,IP=192.16
8.1.129, IP=192.168.001.014,IP=000.000.000.000,ENDC,
NAME=private,VIND=1,TRAP=NO,ACCESS=W,IP=192.168.001.014,
IP=192.168.001.230, IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,IP=000.000.000.
000, IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,IP=000.000.000.
000, IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,IP=000.000.000.
000, IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,IP=000.000.000.
000, IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,IP=000.000.000.
000, IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,IP=000.000.000.
000, IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,IP=000.000.000.
000, IP=000.000.000.000,IP=000.000.000.000,ENDC,
END
```

2. Edit the file by configuring any of the following parameters:
   - GenTraps: set to "YES" if you want SNMP traps to be generated

     If you do not use SNMP on your network, set GenTraps to "NO".

   - Community Names
   - Access: "W" for read/write ("R" = read only)
   - IP Addresses
3. Press **<Enter>** or click the **Submit Changes** button near the bottom of the page.
   The NTS resets, starting up with the new parameters in place.

3.1.8 Leaving the Control Pages

The control session, activated with a successful login, ends under the following circumstances:

- Inactivity: no page navigation or submission of changes in the last five minutes.
- Location change: navigation to a status page or the home page.

If inadvertently logged out, navigate to the **Configuration Control Login** page (by clicking the **Controls** button) from the home page or any status page, then follow the guidelines above.

3.1.9 Leaving the Web Interface

To terminate the web interface, exit your web browser or enter a new URL.

3.2 Telnet Access

The NTS can perform setup and control operations sent from a remote location through the Internet. The protocol used for Internet access to an NTS is Telnet, a standard Internet communications program, with an ASCII character-based interface, that is bundled with Windows 95/98/NT and connects to the NTS through its NET Port. Use Telnet just like Procomm, or any other serial interface program, by entering F-series commands, to which the NTS responds.

The Utility Port takes precedence over the Telnet session. If the Utility Port is active, either Telnet login will fail or, if already logged in, trying to send any Telnet command generates the response:

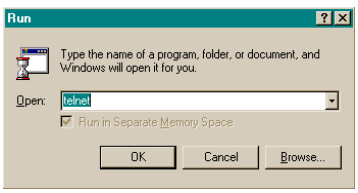
```
NOTICE: Cannot respond to command because Utility Port
session has priority.
```

Telnet sessions have a 15 minute session timer. If there is no activity on the Telnet session, the timer automatically terminates the session.

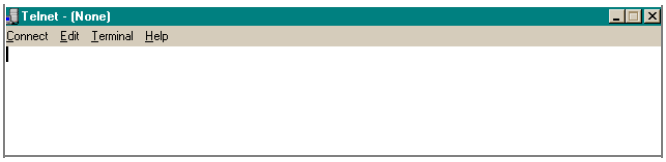
3.2.1 Starting Telnet and Making a Connection

The following section only applies to Microsoft Windows users. If you are using an operating system other than Windows (such as Macintosh or UNIX), check with your System Administrator for Telnet application information.

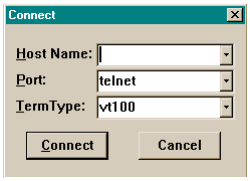
1. Press the Start button at the lower left of your screen.
2. Click **Run** and enter **`Telnet`** in the **Open** field.
   The **Run** dialog box appears:



3. Click **OK**.
   The **Telnet – (None)** window appears:



4. Click **Connect**, the first item on the Telnet menu bar, then select **Remote System**.
   The **Connect** dialog box appears:



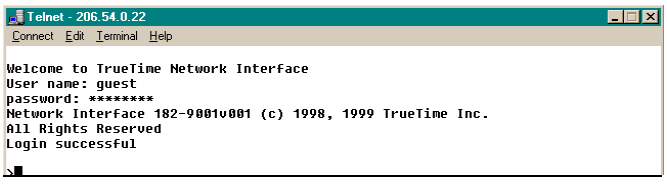
5. In the **Host Name** field, enter the IP Address of the NTS.
   Do not change the text in the other two fields, which should read “Telnet” and “VT100”.

6. Click **Connect** to start a Telnet connection to the NTS.
   If the connection was successful, a login prompt appears:

   If an hourglass appears instead, it means the connection was not successful and you should repeat steps 1-5.

7. Enter the login name **`guest`**.
   A password prompt appears.

8. Enter the default password **`truetime`** (one word, all lower case).
   A welcome message appears if the login and password are approved:



9. Begin your Telnet session by entering F-series commands.

3.2.2 Ending Telnet

There are three ways to end Telnet:

- Close it from your terminal by selecting **Exit** from the **Connect** menu.
- Enter an exit command, such as **`exit`**, or **`quit`**.
- Let it timeout. If no commands are received for 15 minutes, the NTS automatically terminates the session.

3.3 Serial Access

The RS-232 connector provides serial access. The RS-232 connector is located between the NET Port and the front panel display (see Figure 1-1 on page 1-7). This connector is labeled "Serial I/O", and is referred to as the "Utility Port." Table 3-1 below describes the Utility Port's RS-232 pinouts and signal levels.

Serial time output is not available on the Utility Port.

Table 3-1: RS-232 Pinouts and Signal Levels

NTS	9- to 25- PIN ADAPTER CABLE 9-pin 25-pin	SIGNAL DESCRIPTION
OPEN	1 8	DCD, CARRIER DETECT
IN RXD	2– – – – – – <– – – – – – – –3	TRANSMITTED DATA
OUT TXD	3– – – – – – >– – – – – – – –2	RECEIVED DATA
OPEN	4 20	DTR, DATA TERMINAL READY
GND	5– – – – – – <>– – – – – – 7	SC, SIGNAL GROUND
OPEN	6 6	DSR, DATA SET READY
OPEN	7 4	RTS, REQUEST TO SEND
OPEN	8 5	CTS, CLEAR TO SEND
OPEN	9 22	RI, RING INDICATOR

3.3.1 Serial Line Settings

Serial I/O settings are factory set and cannot be changed. The default serial format is:

Data Rates: **9600 bits/second**

Word Length: **8 bits**

Parity: **None**

Stop Bits: **1**

The Utility Port can be connected either to a terminal or to a computer, using a null modem cable, and used in conjunction with any serial access (terminal emulation) software program, such as Procomm or HyperTerminal. The following section illustrates a terminal connection, using HyperTerminal, a popular Windows-based application. All commands are input using conventional TrueTime F-series type commands (see “Command List” on page 4-3).

These examples apply *only* to systems using Windows 95/98/NT. Check with your System Administrator if you are using a different operating system (such as Macintosh or UNIX).

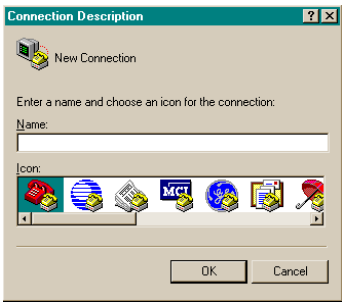
3.3.2 HyperTerminal

Starting HyperTerminal

To start HyperTerminal:

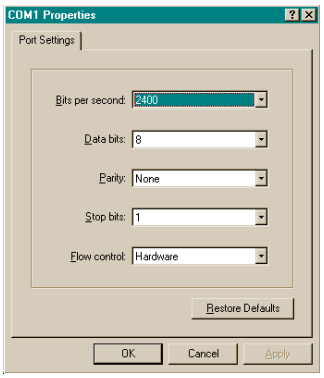
1. Click the **Start** button on the task bar.

2. Select **Programs > Accessories > HyperTerminal > HyperTerminal**. The **Connection Description** dialog box appears:



3. Enter a name (such as “NTS”) for this connection in the **Name** box and click **OK**. The **Connect To** dialog box appears:

4. In the **Connect using** box, use the drop-down menu to select your modem's Com port (COM1 in this example), then click **OK**.
   The **COM1 Properties** dialog box appears, showing the **Port Settings** tab:



5. Edit the fields in the **Port Settings** dialog box as follows:

   Bits per second: **9600**

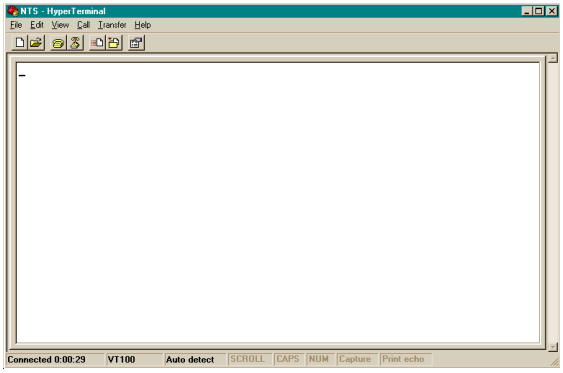
   Data Bits: **8**

   Parity: **None**

   Stop Bits: **1**

   Flow control: **None**

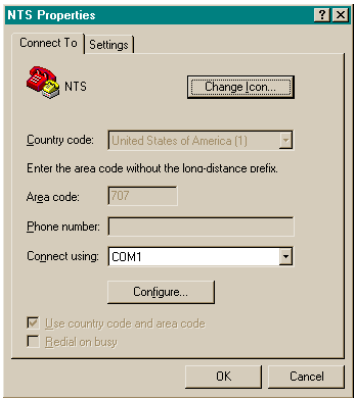
6. Click **OK**.
   The **NTS HyperTerminal** window appears, indicating the NTS is now connected through the Utility Port:



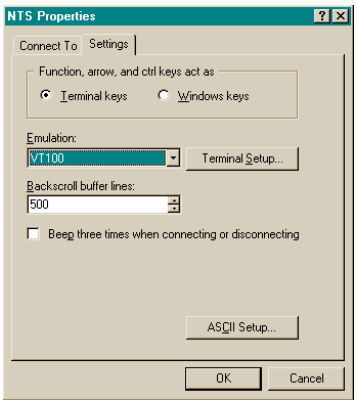
Setting Up a HyperTerminal Session

To set up a HyperTerminal session:

1. From the **File** menu in the session window, select **Properties**.
   The **NTS Properties** dialog box appears, showing the **Connect To** tab:

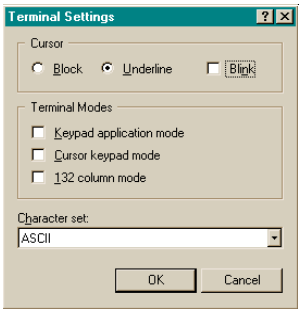


2. Select the **Settings** tab and click the **Terminal keys** radio button:



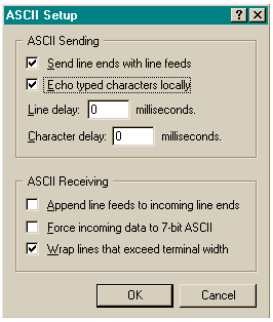
3. In the **Emulation** box, use the drop-down menu to select **VT100** terminal type (do not select the **Auto detect** option).

4. Click **Terminal Setup** and configure the terminal by selecting the appropriate options in the **Terminal Settings** dialog box (with a VT100 terminal, the recommended settings are pictured below):



5. Click **OK**.
   The **NTS Properties** dialog box is reactivated.

6. In the **NTS Properties** dialog box, click **ASCII Setup**…
   The **ASCII Setup** dialog box appears:



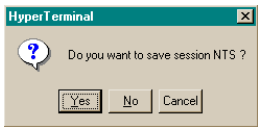
7. Place check marks in the following boxes:

   - Send line end with line feeds
   - Wrap lines that exceed terminal width

8. Click **OK**.
   This returns you to the **NTS Properties** dialog box.

9. Click **OK**.
   This returns you to your HyperTerminal session window, where you can enter "F" series commands. Press the **Return** key to get a > prompt.

10. When exiting HyperTerminal, click **Yes** when prompted to save the current session:



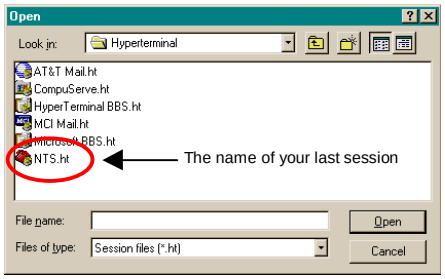
The next time you launch HyperTerminal from the **Start** menu, you can reconnect to the session you just created.

Reconnecting to your last HyperTerminal session

To reconnect to your last HyperTerminal session:

1. From the **HyperTerminal** window, select **File > Open**.

2. Double-click your last session:



3.4 Session Timers

There are timers on Utility Port, Telnet, and web control sessions that terminate them if there is a lack of activity. Any action you take during a session automatically resets the timer, and it starts all over again. The timers and their interactions are described below.

3.4.1 Utility Port Session Timer

The Utility Port Session Timer starts upon receipt of a character from the Utility Port. The timer is reset upon receipt of every character. If no characters are received for 15 consecutive minutes, the session terminates.

When a Utility Port Session is in progress, Telnet cannot execute any commands to the NTS. The Utility Port Session must end before full Telnet access is possible.

3.4.2 Telnet Session Timer

The Telnet Session Timer starts upon receipt of a command line from Telnet, via the NET Port. The timer is reset upon receipt of every command line. If no lines are received for 15 consecutive minutes, the session terminates.

Terminating a Telnet session drops the connection to the remote host. You can immediately activate a new session by re-connecting and logging in again.

3.4.3 Web Control Session Timer

Once you are logged in to any Control Page, you can send HTTP requests from a web browser, via the NET Port. The Web Control Session Timer starts as soon as it receives such a request. The timer is reset upon receipt of every HTTP request. If no HTTP requests are received for five consecutive minutes, the session terminates.

Terminating a Web Control session causes the NTS to deny any further requests you make for changes. You can immediately activate a new session by logging in again.

4

Serial or Telnet I/O Functions

4.1 Overview and Format

Shortly after power-up, the utility port will be ready to receive commands. To ensure the unit receives data input accurately, wait until the message `Searching for Satellites...` has been on the front panel before entering any serial or Telnet commands.

You can send data to, or request data from, the unit by sending serial or Telnet commands using ASCII character strings. The general form of these commands is:

F<FUNC#><Enter>

where:

F	=	ASCII character F
<FUNC#>	=	two-digit function number
<Enter>	=	input line terminator

More specifically, the data input and output formats are:

F<FUNC#>[<SP><FIELD>]<Enter> (input)

or

`F<FUNC#>[<SP><FIELD>]<CR><LF>` (output)

where:

F	=	ASCII character F
<FUNC#>	=	function number
<SP>	=	space
<FIELD>	=	data entry or request
<CR><LF>	=	output line terminator
[ ]	=	encloses a phrase that is repeated as often as necessary

Output strings are kept to fixed lengths whenever possible. This means that numeric values often contain many leading blanks. This user's guide represents output strings in a fixed font. For example:

```
F60 prn 14 good enabled sig level= +21.37<CR><LF>
```

The formats of the output strings are designed so that it is possible to request the state of a function and save the response string. Later that string can be sent to the unit to restore the original state of that function.

Input strings sent to the unit may vary in length. The manual represents what you should type in the same fixed font, with a bold typeface. It represents the necessary keyboard action differently, however, as per the manual conventions (page 1-1). For example:

F03<**Enter**>

The number of separators between fields may vary. You can enter numeric values with or without leading zeros. When entering positive quantities, you can omit the plus sign.

String fields (such as “on” or “off”) may be entered in upper or lower case, as can the “F” that starts all serial or Telnet commands. Some fields of some commands are optional and may be replaced by a semicolon. In that case, the corresponding value is unchanged.

End all input strings by pressing the **<Enter>** or **<Return>** key on your keyboard.

An incorrect entry may result in an error message, as described in “Error Messages” on page 5-1. The unit responds to correct entries with:

OK<CR><LF>

In addition to the regular F-series commands, there is also a set of F100 commands, known collectively as Extended Function Commands. With certain F100 commands, you can reconfigure network parameters, such as IP Address, or modify function settings like Remote Lockout. These commands include F100 BASET, IP / SM / G / CONFIG (“set” commands) / DHCP and LOCK. Changes to any of these settings, except F100 LOCK, cause the unit to reset automatically.

After making changes to values in any of these parameters/functions, a confirmation prompt appears (“Are you sure?”). For safety, the default response to this prompt is negative. The unit will not execute the command unless you respond affirmatively by entering the letter “y” within 10 seconds. Within that time period, any other response, including no response, results in the unit canceling the command.

4.2 Command List

The following table lists all serial/Telnet commands that are used to operate, administer, and maintain the unit. The Utility Port is ready to receive these commands once the power-up sequence is complete. The F100 series is used mainly to request or set unit NET Port parameters. Configuration of the IP Address, Subnet Mask, Default Gateway, and DHCP parameters is also available through the front panel keypad. Changing any network parameter causes the unit to reboot.

Use the front panel keypad to set initial system configuration values at first installation.

Table 4-1: F-Series Function Commands

Command	Function	Parameters
F03	Time/Date Request	MM/DD/YYYYHH:MM:SS
F18	Software Version Request	– (equivalent to F100 VER)
F36	Network Configuration Entry/Request	EA, IP, SM, G (equivalent to corresponding F100 commands)
F53	Operating Mode Request	–
F60	Satellite List Request	–
F67	Leap Second Information Request	–
F72	Fault Status Request	–
F100 BASET	100Base-T/10Base-T Entry/Request	10, 100 (change requires confirmation within 10 seconds)
F100 DHCP	DHCP Control	ENABLE/DISABLE (change requires confirmation within 10 seconds)
F100 EA	Ethernet Address	–
F100 IP	IP Address	### ### ### ### (change requires confirmation within 10 seconds)
F100 SM	Subnet Mask	### ### ### ### (change requires confirmation within 10 seconds)
F100 G	Default Gateway	#### #### #### #### (change requires confirmation within 10 seconds)
F100 IC	Network Configuration Request	IP, SM, G
F100 P	Password Change Request	XXXXXXX
F100 ST	Self Test Results Request	–
F100 VER	Software Version Request	–
F100 CONFIG	NTP and SNMP Configuration	“GET” , “SET”, “NTP”, “SNMP”, “IP ADDRESS”, “YES”, “NO”, “W”, “R” (change requires confirmation within 10 seconds)
F100 LOCK	Remote Lockout	LOCK (change requires confirmation within 10 seconds)
F100 L	Lock Display Request	–

Additional F100 Extended Function commands are available for updating software, changing passwords, pinging remote units, and displaying UTC time in seconds.

Table 4-2 F-Series Additional F100 Extended Function Commands

Command	Function	Parameters
F100 J	Jumper Setting Request	–
F100 BH	Burn Host	FTP host address, file path, file name
F100 BU	Burn	–
F100 BUB	Burn BootLoader	–
F100 BF	Burn File System	–
F100 BL	Burn Host Lock Request	–
F100BLS	Burn Host Lock Set	(change requires confirmation within 10 seconds)
F100 BLR	Burn Host Lock Reset	(change requires confirmation within 10 seconds)
F100 K I L L	Reboot	–
F100 PN	Password System User Name Change	XXXXXXX
F100 PR	Password Reset	(change requires confirmation within 10 seconds)
F100 PRESETALL	Password Reset All	(change requires confirmation within 10 seconds)
F100 PL	Password Lock Request	–
F100 PLS	Password Lock Set	(change requires confirmation within 10 seconds)
F100 PLR	Password Lock Reset	(change requires confirmation within 10 seconds)
F100 PE LIST	Peer List	–
F100 PE ADD	Peer Add	IP address
F100 PE REM	Peer Remove	IP address
F100 PI	Ping Request	IP address
F100 PT	Time Request	–

Function commands and unit responses contain common elements which are defined in the following table:

Table 4-3: Definitions of Common Elements in Serial Commands and Responses

Element	Definition
<CR><LF>	Line terminator, a carriage return (0x0D) and line feed (0x0A)
<SP>	One or more separator characters: either space (0x20), comma (0x2C), or tab (0x09)
±	Either no character, + (0x2B), or - (0x2D)
<HH>	Two digit hour, 0-23
<MM>	Two digit minutes, 0-59
<SS>	Two digit seconds, 0-59
<yyyy>	Four Digit Year, 0-9999
<dd>	Two Digit Day of month, 1-31
<DDD>	Three Digit Day of Year, 1-366
<mm>	Two Digit Month, 1-12
<SOH>	ASCII Start-of-Header character (HEX 01).
<mmm>	Three Digit milliseconds

4.3 Function Commands

4.3.1 F03 – Time and Date Request

Use Function F03 to request time and date. The response is UTC date and time.

To request TIME AND DATE, send the following command:

F03<**Enter**>

The unit responds:

F03<SP><mm>/<dd>/<yyyy><SP><HH>:<MM>:<SS><CR><LF>

where

F	=	ASCII character F
03	=	function number
<SP>	=	space
<mm>	=	one- or two-digit month
/	=	ASCII character slash
<dd>	=	one- or two-digit day
<yyyy>	=	four-digit year (if you manually entered this data)
<HH>	=	one- or two-digit hours
:	=	ASCII character for a colon
<MM>	=	two-digit minutes
<SS>	=	two-digit seconds
;	=	replacement character
<Enter>	=	input line terminator
<CR><LF>	=	output line terminator

Sample Entry: **F03**<**Enter**>

The response might be: F03 UTC 01/07/1996 02:48:29<CR><LF>

4.3.2 F18 – Software Version Request

Use Version Request to query the software version number of the unit. The version number is factory set and cannot be changed. This command is for backwards compatibility and is identical to the F100 VER command (see page 4-18).

4.3.3 F36 – NET Port Network Configuration Entry/Request

Use Function F36 to request or set network parameters. Changes require the unit to reset. F36 commands are for backward compatibility and are identical to the F100 function command series used for the same purpose (see the sections starting on page 4-11).

F36 commands are for backward compatibility with previous TrueTime products. F36 and F100 commands can both be used to query or change specific NET Port network parameters.

The F36 EA (and F100 EA) command reports in the Ethernet address IEEE format, which may result in numbers which differ from those reported by your system. Since the Ethernet address is a fixed value, as long as the unit is up and running (you can ping the unit to be sure), you can safely ignore these differences.

4.3.4 F53 – Operating Mode Request

Use Function F53 to verify the number of satellites currently being tracked. F53 also reports the unit's operating mode, which is always Survey Static.

To see the number of tracked satellites, send the following command:

F53<Enter>

The unit responds:

```
F53<SP><MODE>:<SP><#><SP>SATS<CR><LF>
```

where

F	=	ASCII character F
53	=	function number
<SP>	=	space
<MODE>	=	SURVEY STATIC
:	=	ASCII colon
<#>	=	number of satellites being tracked
<Enter>	=	input line terminator
<CR><LF>	=	output line terminator

Sample entry: **F53<Enter>**
The response might be: `F53 SURVEY STATIC SATS: 6<CR><LF>`

4.3.5 F60 – Satellite List Request

Use Function 60 to list current satellites and to see the relative signal strength of satellites the unit is tracking. Signal strength is given in units in the range of 0 to +25.

The unit monitors five variables: the prn number, good/bad, enabled/disabled, tracked, and current.

To request the list, send the following command:

F60<Enter>

where

F	=	ASCII character F
60	=	function number
<Enter>	=	input line terminator

The unit responds:

```
F60<SP>prn NN<SP>good<SP>enabled<SP>tracked<SP>current<SP>
sig<SP>level<SP>= +<LEVEL><CR><LF>
```

where

prn NN	=	pseudo-random number; the prn number is a unique identifier for a particular satellite's communication path; for example, satellite 3 might have the prn number 15; if that satellite is recalled to Earth and replaced by satellite 42, the communication path of satellite 42 might also be assigned prn 15
enabled/disabled	=	"Enabled" refers to a factory default configuration value that allows the GPS to track all satellites on the F60 list
good/bad	=	"Good" means all three of the following apply: • the satellite is visible, *and* • the satellite's ephemeris and almanac data report the satellite's health as "good", *and* • the satellite reports its own health as "good" "Bad" means at least one of the following applies: • the satellite is not visible, *or* • the satellite's ephemeris and almanac data report the satellite's health as "bad", *or* • the satellite reports its own health as "bad" (for example, during maintenance periods)
tracked	=	"Tracked" means that the unit is tracking this particular satellite
current	=	"Current" means that the unit is both tracking this satellite *and* using the satellite's communication to calculate accurate time; an example from the list is prn 3
<CR><LF>	=	line terminator

You can see from the sample list below that “enabled”, “good”, and “tracked” satellites are “current”. That means that the unit does not use any satellite with questionable communication to calculate time, even if that satellite is enabled, visible and being tracked.

Sample entry: **F60<Enter>**

The response is a current list, an example of which is:

```
F60 prn 1  bad  enabled                sig level= +0.00
F60 prn 2  bad  enabled                sig level= +0.00
F60 prn 3  good enabled tracked current sig level=+13.64
F60 prn 4  bad  enabled                sig level= +0.00
F60 prn 5  bad  enabled                sig level= +0.00
F60 prn 6  good enabled                sig level= +0.00
F60 prn 7  bad  enabled                sig level= +0.00
F60 prn 8  bad  enabled                sig level= +0.00
F60 prn 9  bad  enabled                sig level= +0.00
F60 prn 10 bad  enabled                sig level= +0.00
F60 prn 11 bad  enabled tracked        sig level= +3.00
F60 prn 12 bad  enabled                sig level= +0.00
F60 prn 13 bad  enabled                sig level= +0.00
F60 prn 14 bad  enabled                sig level= +0.00
F60 prn 15 good enabled tracked current sig level=+22.77
F60 prn 16 bad  enabled                sig level= +0.00
F60 prn 17 good enabled                sig level= +0.00
F60 prn 18 bad  enabled                sig level= +0.00
F60 prn 19 bad  enabled                sig level= +0.00
F60 prn 20 bad  enabled tracked        sig level= +3.00
F60 prn 21 good enabled tracked current sig level=+20.15
F60 prn 22 good enabled                sig level= +0.00
F60 prn 23 good enabled tracked current sig level=+15.27
F60 prn 24 bad  enabled                sig level= +0.00
F60 prn 25 bad  enabled tracked        sig level= +3.47
F60 prn 26 good enabled                sig level= +0.00
F60 prn 27 bad  enabled                sig level= +0.00
F60 prn 28 bad  enabled                sig level= +0.00
F60 prn 29 good enabled tracked current sig level=+21.46
F60 prn 30 bad  enabled                sig level= +0.00
F60 prn 31 good enabled tracked current sig level=+18.10
F60 prn 32 bad  enabled                sig level= +0.00
```

4.3.6 F67 – Leap Second Information

Use Function 67 to retrieve information regarding upcoming leap seconds. This is satellite information and *cannot* be changed through the unit. Although UTC leap second adjustments may be performed on four occasions annually, in practice they are only performed twice: June 30th and December 31st.

To return the leap second status, send the following command:

F67<Enter>

where

F	=	ASCII character
F	=	function number
<Enter>	=	input line terminator
<CR><LF>	=	output line terminator

An example of the response might be:

```
F67 06/30/96 +1 <CR><LF>
```

This response indicates there is a leap second addition during the last minute of June 30, 1996.

If there was no leap second pending, the response might be:

```
F67 none <CR><LF>
```

4.3.7 F72 – Fault Status Request

Use Function F72 to display the status of the antenna feed circuit, and GPS lock status fault detectors within the unit.

To display the status of the fault detectors, send the following command:

F72<Enter>

The unit responds:

```
F72<SP>Antenna: <ANT STATUS> GPS: <GPS STATUS><CR><LF>
```

where:

F	=	ASCII character F
72	=	function number
<SP>	=	space
<ANT STATUS>	=	OPEN, GOOD or SHORTED
<GPS STATUS>	=	LOCKED, UNLOCKED
<CR><LF>	=	output line terminator

Sample entry: **F72<Enter>**
The response might be: `F72 Antenna: OK GPS: Locked<CR><LF>`

4.4 Extended Function Commands

The F100 command series is known collectively as Extended Function Commands. With certain F100 commands, you can reconfigure network parameters, such as IP Address, or modify function settings like Remote Lockout. The main commands include F100 BASET, IP / SM / G / CONFIG ("set" commands) / DHCP, LOCK, UNLOCK and L. Changes to any of these settings, except F100 LOCK, cause the unit to reset automatically after you respond to a confirmation prompt. Other commands are available for changing passwords (PN, PR, PRESETALL, PL, PLS, PLR) and updating software (J, BH, BU, BUB, BF, BL, BLS, BLR), as well as pinging remote hosts (PI) and displaying UTC time in seconds (PT).

For safety, the default response to the confirmation prompt is negative. The unit will not execute the command unless you respond affirmatively (enter the letter "y") within 10 seconds. Within that time period, any other response, including no response, results in the unit canceling the command.

In those sections below where it is not already stated, **<Enter>** = input line terminator and <CR><LF> = output line terminator.

F100 Command Configuration Notes:

- **Network parameters can be queried at any time, but cannot be changed unless DHCP is disabled first.**
- **You can reconfigure two or more network parameters in a single entry by sending the F100 command and entering new values. You will have to respond (within 10 seconds) to separate confirmation prompts for each value that you change.**
- **Leading zeros may be omitted when entering IP Address, Subnet Mask, and Default Gateway.**
- **Any field may be omitted and order is not significant.**
- **Blanks are allowed on either side of a colon.**
- **The unit reboots after any network parameter is changed.**

4.4.1 F100 BASET – 100 BASE-T/10 BASE-T Control

Use the BASET command to query the current Base-T setting. If you set the unit to 10Base-T, it operates only at that speed. If you set the unit to 100Base-T, it negotiates between 10/100Base-T. This does not necessarily mean the unit will connect at 100Base-T, but will connect at the fastest possible speed. Any change to the current Base-T setting causes the unit to reset.

To query the maximum Base-T speed, send the following command:

F100<SP>BASET<Enter>

where

F	=	ASCII character F
100	=	unit function number
<SP>	=	space
BASET	=	specify Base-T command
<Enter>	=	input line terminator

An example of the response is:

```
F100 BASET 100T
```

To set the maximum connection speed to 100Base-T, send the following command:

F100<SP>BASET<SP>100<Enter>

where:

100	=	set maximum Base-T speed to 100

To set the maximum connection speed to 10Base-T, send the following command:

F100<SP>BASET<SP>10<Enter>

where

10	=	set maximum Base-T speed to 10

In both these cases, the unit responds:

```
Are you sure? (y/N)
```

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

For details about an initial 100Base-T setting, see “NET Port Network Parameters: First Time Configuration” on page 2-7.

4.4.2 F100 DHCP – DHCP Control

Use F100 DHCP to enable or disable Dynamic Host Configuration Protocol. DHCP allows the unit to auto-configure its network address, provided that you have enabled DHCP, and that the unit is installed on, *and connected to at power-up*, an Ethernet LAN with a DHCP server. If these conditions are not met, the unit reverts to those network parameters in use at the last power-down. By default, DHCP is off at initial installation.

Disable DHCP before changing any Network parameter. Changing DHCP status causes a software reset of the unit. DHCP status can be *queried* without rebooting the unit.

To enable DHCP, send the following command:

F100<SP>DHCP<SP>ENABLE<Enter>

where:

F	=	ASCII character F
100	=	unit function number
<SP>	=	space
DHCP	=	specify DHCP command
ENABLE	=	command DHCP to be enabled
<Enter>	=	input line terminator

To disable DHCP, send the following command:

F100<SP>DHCP<SP>DISABLE<Enter>

where:

DISABLE	=	command DHCP to be disabled

The unit responds:

```
Are you sure? (y/N)
```

As a safety feature, after sending this command you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

To query the status of DHCP send:

F100<SP>DHCP<Enter>

An example of the response is:

```
F100 DHCP OFF
```

4.4.3 F100 EA – Ethernet Address

The Ethernet address is assigned at the factory. It is a fixed, six-byte, hexadecimal value specific to the unit NET Port. The first three bytes are registered to TrueTime Inc.; the last three bytes are the hex value identifying the NET Port.

To request the Ethernet address of the unit NET Port, send the following command:

F100 EA<**Enter**>

The unit responds:

F100 EA:00-A0-69-xx-xx-xx<CR><LF>

where "xx-xx-xx" are the six hex digits of the unit's unique address.

An example of the response is:

F100 EA:00-A0-69-00-06-2A

Attempts to set this field will be rejected with a syntax error message.

The F100 EA (and F36EA) command reports in the Ethernet address IEEE format, which may result in numbers which differ from those reported by your system. Since the Ethernet address is a fixed value, as long as the unit is up and running (you can ping the unit to be sure), you can safely ignore these differences.

4.4.4 F100 IP – IP Address

To obtain the IP address of the unit NET Port, send the following command:

F100 IP<**Enter**>

The unit responds:

F100 IP:nnn.nnn.nnn.nnn<CR><LF>

where "nnn.nnn.nnn.nnn" is the dotted decimal address notation.

An example of the response is:

F100 IP:206.54.0.33

Changing the IP Address requires the unit to reset. A verification prompt appears prior to execution.

To set the IP address and restart the unit, send the following command:

F100 IP:nnn.nnn.nnn.nnn<**Enter**>

Sample entry: **F100 IP:206.54.0.21**<**Enter**>
The response is: Are you sure? (y/N)

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter "y") to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

4.4.5 F100 SM – Subnet Mask

To return the subnet mask of the NET Port, send the following command:

F100 SM<**Enter**>

The unit responds:

F100 SM:nnn.nnn.nnn.nnn<CR><LF>

An example of the response is:

F100 SM:255.255.255.125

Changing the Subnet Mask requires the unit to reset. A verification prompt appears prior to execution.

To set the subnet mask and restart the unit, send the following command:

F100 SM:nnn.nnn.nnn.nnn<**Enter**>

Sample entry: **F100 SM:255.255.255.240**<**Enter**>
The response is: Are you sure?(y/N)<CR><LF>

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter "y") to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

4.4.6 F100 G – Gateway

To obtain the Default Gateway of the unit NET Port, send the following command:

F100 G<**Enter**>

The unit responds:

F100 G:nnn.nnn.nnn.nnn<CR><LF>

An example of the response is:

F100 G:206.54.0.1

Changing the Default Gateway requires the unit to reset. A verification prompt appears prior to execution.

To set the Default Gateway and restart the unit, send the following command:

F100 G:nnn.nnn.nnn.nnn<**Enter**>

Sample entry: **F100 G:206.54.0.17**<**Enter**>
The response is: Are you sure?(y/N)<CR><LF>

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter "y") to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

4.4.7 F100 IC – NET Port Network Configuration Entry/Request

To review the entire NET Port network configuration, send the following command:

F100<**SP**>**IC**<**Enter**>

An example of the response is:

```
F100 IP:206.54.0.21 SM:255.255.255.240
G:206.54.0.17N:E<CR><LF>
```

where N:E denotes Ethernet DIX.

4.4.8 F100 P – Change User Password

If you want to change a password, you must log in as the user for whom you want to change the password (also see page 4-36). The maximum password size is ten characters.

To change the user password, send the following command:

F100<**SP**>**P**<**Enter**>

where:

F	=	ASCII character F
100	=	unit function number
<SP>	=	space
P	=	specify Password command
<Enter>	=	input line terminator

The unit responds:

```
Enter new user password:
```

When you enter a new password, the unit responds with:

```
Enter it again:
```

Enter the same new password again, to confirm the spelling. If the same new password has been entered twice, the unit responds with:

```
OK<CR><LF>
```

In this case, the new password will be used for the next login (serial or Telnet). However, if the new password is entered differently the second time, the unit responds with:

```
ERROR: Passwords do NOT match.  New password rejected.
```

In this case, the old password will be used for the next login (serial or Telnet).

If you have forgotten your user name and/or password, you can go into bootloader mode and reset them. In bootloader mode the unit recognizes the default user name and password. You can then use F100 PR (see page 4-32) or F100 PRESETALL (see page 4-31) to change the user name and password to defaults for use in the normal mode, or you can use F100 PN (see page 4-32) and F100 P (the above command) to

change the user name and password to whatever you want. Then you can go back into normal mode the and the user name and password you just set will work.

4.4.9 F100 ST – Self Test Status

Use Self Test Status to query the status of the power-up tests. The response contains the PASS/FAIL status of the flash memory checksum test, RAM test, Utility Port test, and version check.

To query the self-test status, send the following command:

F100<SP>ST<Enter>

where:

F	=	ASCII character F
100	=	unit function number
<SP>	=	space
ST	=	specify ST command
<Enter>	=	input line terminator

The unit responds:

```
F100<SP>ST<SP>FLASH/CRC<SP>:<SP><STATUS>,<SP>RAM<SP>:
<SP><STATUS>,<SP>SERIAL<SP>:<SP><STATUS>,<SP>VER<SP>:
<SP><STATUS><CR><LF>
```

where:

F	=	ASCII character F
100	=	unit function number
<SP>	=	space
ST	=	specify ST command
FLASH/CRC	=	specify flash checksum result
RAM	=	specify RAM test result
SERIAL	=	specify Utility Port test result.
VER	=	specify version test result. This test compares the version of the code against the version recorded in Non-Volatile memory
<STATUS>	=	is either ASCII PASS or FAIL
,	=	ASCII comma
:	=	ASCII colon
<CR><LF>	=	output line terminator

An example of the response is:

```
F100 ST flash/CRC : PASS, Ram : PASS, Serial : PASS, Ver :
PASS<CR><LF>
```

4.4.10 F100 VER – Software Version Request

Use Version Request to obtain the software version number of the unit. The version number is set at compile time, and cannot be changed. It may only be queried.

To query the version number send the following command:

F100<SP>VER<Enter>

where:

F	=	ASCII character F
100	=	unit function number
<SP>	=	space
VER	=	specify Version Request command
<Enter>	=	input line terminator

An example of the response is:

```
f100 VER <CR><LF>
Bootloader  182-9003V000<CR><LF>
Software    182-9004V000<CR><LF>
File System 182-9005V000
Serial #    102578

Software:   NTS-200
    Date:   May 19, 2001, 02:27:13
```

4.4.11 F100 CONFIG – FTP Configuration of NTP & SNMP Parameters

Although you can change the NTP and SNMP parameters contained in the `temp/directory` through FTP and a text editor, it is much faster and easier to do this over the Internet (see "Network Control Page" on page 3-3 for details).

For more information about NTP and NTP broadcast mode, see Appendix A and Appendix B. For details on SNMP, see Appendix D.

Installing and Using FTP Software

If you choose the F100 CONFIG option, you need an FTP server, which is any server that supports Anonymous FTP. If you do not have an FTP server available, you can turn your own Windows workstation into an FTP server by running any ftpdaemon software that is available on the Web. Follow the instructions that come with your ftpdaemon software to set it up. The software needs to allow anonymous login and allow uploads.

Once the software is set up you can login to the unit through a serial/Telnet interface.

To configure NTP and SNMP parameters, use "get" and "set" commands. Both these commands have the same general format:

F100<SP>CONFIG<SP><ACTION><SP><TYPE><SP>HOST:<IPADDRESS><SP>DIR:<DIRECTORY><Enter>

where:

F	=	ASCII character F
100	=	unit function number
<SP>	=	space
CONFIG	=	specifies configuration command
<ACTION>	=	specifies the action to be taken: either GET to retrieve data from the unit, or SET to send the modified data back to the unit
<TYPE>	=	specifies the type of file to be used, NTP or SNMP
<HOST:IPADDRESS>	=	your IP Address (the FTP host)
DIR:<DIRECTORY>	=	the directory on your C drive where you want the data to reside.
<Enter>	=	input line terminator

Use a “get” command to retrieve data from the unit and have it delivered, through the FTP software, to a specified directory on your C drive. You must use the UNIX format with forward slashes to specify your IP address and the target directory. The FTP software delivers the data in a configuration file. Once this file is in the directory, use any text editor to modify it.

In a “get” command line, you can enter the elements “ntp”, “snmp”, and “get” in any order. If you want to configure both NTP and SNMP at the same time, place both elements in the command line.

Use a “set” command to transfer the modified data from the configuration file in your directory back to the unit. Once again, you must specify your IP address and the directory on your hard drive that contains the configuration file. “Set” commands cause the unit to reboot. A confirmation prompt appears, to which you must respond affirmatively (“y”) within 10 seconds, before the unit executes the command and resets.

In a “set” command line, you can enter the elements “ntp”, “snmp”, and “get” in any order. If you want to configure both NTP and SNMP at the same time, place both elements in the command line.

Configuration of NTP Parameters Using FTP

To configure NTP parameters using FTP and a text editor, follow the steps outlined below. However, it is much faster and easier to do this over the Internet (see "Remote NTP Configuration" on page 3-4). During this process, the FTP software creates default configuration files ("ntp.conf" and "ntp.keys") in your directory to hold the data you have requested. Do *not* change the names of these files.

The unit does not support NTP client mode. Any "server" settings in ntp.conf will be ignored.

1. Send a "get" command: **`F100 config get ntp host:192.168.1.14 dir:temp`**

The unit responds:

```
Host config ip 192.168.1.14 configured
successfully!
Source file/etc/ntp.conf bytes read: 70
Dest File temp/ntp.conf bytes written: 70
Source file/etc/ntp.keys bytes read: 70
Dest File temp/ntp.keys bytes written: 70
Configuration files transferred successfully!
```

An example "ntp.conf" file might look like:

```
# Note= ALL servers are optional.  If your GPS antenna is
connected and positioned correctly, the servers listed here are
not used.  These servers are used only when the GPS unit fails.
GPS failure is detected automatically.  Note that when the NTS is
using these timeservers the system is, at best, running with 20
millisecond precision.  Up to 10 NTP servers can be assigned in
this file.  The addresses below are examples, and should be
changed as required by your network configuration.

The following are public TrueTime NTP Timeservers.  Uncomment
one or both to enable NTP fallback to TrueTime if GPS
synchronization is lost.  Add any other server address.
#
server     206.54.0.20
server     206.54.0.21

Private time servers (example only).

server     192.168.1.35

# Uncomment the "broadcast" line below to enable NTP broadcast
mode with MD5
# using key 1. The key may be omitted, but is less secure.  If a
key is used here, a corresponding entry for that key must appear
in the NTP key file.  A maximum of 20 keys for broadcast can be
defined on this line.

broadcast     192.168.1.255     key 1
```

```
The line below lists the currently trusted keys. See the NTP keys
file for the actual keys and their corresponding key numbers.
Keys 1 and 2 are listed as an example.  All keys listed must
appear in the NTP keys file.  Note= to ensure maximum security,
remember to change the keys on a regular basis.  A maximum of 20
trusted keys can be defined on this line.

trustedkey     1     2
```

2. Edit the data in the “ntp.conf” file by adding or renaming servers from this list.

3. Edit the data in the “ntp.keys” file (see below).

4. Return the revised data to the unit by sending a “set” command:

`F100 config set ntp host:192.168.1.14 dir:temp`

The unit responds:

```
Are you sure? (y/N)
```

If you answer “y”, the unit responds as follows, then resets:

```
Source file temp/ntp.conf bytes read: 70
Dest File/etc/ntp.conf bytes written:  70
Source file temp/ntp.keys bytes read: 70
Dest File/etc/ntp.keys bytes written:  70
Configuration files transferred successfully!
```

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

When sending a “set” command, the last number in the unit response (“70” in this example) represents file length. Depending on the parameters you configure, this number may vary.

Editing the MD5 keys on the NTP Server

NTP keys are needed if you are using NTP in broadcast mode with MD5 authentication. This (and the following) section provide configuration guidelines. For a discussion of using NTP in broadcast mode without MD5 authentication, see Appendix B.

The Broadcast mode adjusts its periodicity according to feedback from its broadcast client. The periodicity will typically settle-out to about every 2 minutes. This activity is not adjustable.

MD5 private keys have to be edited on both the NTP server and the NTP client. The private keys are defined in the “ntp.keys” file.

The NTP client "ntp.keys" file is identical to the one on the NTP server. For the specific keys used by the NTP server, the NTP client must have the identical line in its version of the file. You'll want to use your own hard-to-guess key names, using random letters. The critical lines of the "ntp.keys" file are:

```
Id    M    Value
----  ---  --------
1     M   truetime
2     M   xyz123
```

where 1 and 2 are key identifiers.

The first column is the key identification number, which may range in whole positive numbers from 1 to 65,535. The second column is the type of key, which is always set to the letter *M* when using MD5 authentication. The third column is the private key that is ASCII text from 1 to 32 characters in length.

For maximum security, use a unique combination of 32 letters and numbers for each key identifier. For correct configuration, do not use zero as a key identifier. Zero means the key identification will not be used.

Editing the MD5 keys on the NTP Client

For NTP client authentication, the line `trustedkey 1 2` in the "ntp.conf" file is required to enable the private keys 1 and 2 from the "ntp.keys" file. The line `bclient` is required for broadcast time packets to be processed by the NTP client. In this case, sample information from a client "ntp.conf" file might look like:

```
trustedkey  1      2
bclient
```

Sample information in a client "ntp.keys" file might look like:

```
1     M     truetime
2     M     longshot
```

When you invoke the NTP client at the command line, use the following options:

- `-b`
  to turn on broadcast reception
- `-k /etc/ntp.keys`
  to specify the name and location of the keys file
- `-d`
  for debugging.

An example command line might look like:

```
ntpd -d -d -d -b  -k /etc/ntp.keys
```

After configuring all MD5 keys, carry out step 4 in the configuration procedure outlined above.

Configuration of SNMP Parameters Using FTP

By default, SNMP is disabled. To use it, or to configure any other SNMP parameter using FTP and a text editor, follow the steps outlined below. However, it is much faster and easier to do this remotely, using the web interface (see "Remote SNMP Configuration" on page 3-6). During this process, the FTP software creates a default configuration file ("snmp.conf") in your directory to hold the data you have requested. Do *not* change the name of this file.

1. Send a "get" command:

Sample Entry: **`F100 config get snmp host:192.168.1.14 dir:temp`**

The unit responds:

```
Source file /config/snmp.conf bytes read: 1274
Dest File  temp/snmp.conf bytes written: 1274
Configuration files transferred successfully!
```

An example "snmp.conf" file might look like the following, with each string appearing as a single line on your display:

```
MIB=/config/ttmib.o,
GenTraps=NO,
sysContact=TrueTime Inc. 707-528-1230,
sysName=NTS-200,
sysLocation=Santa Rosa CA 95407,
NAME=public,VIND=1,TRAP=YES,ACCESS=R,IP=192.168.001.230,
IP=192.168.1.129,IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=private,VIND=1,TRAP=YES,ACCESS=W,IP=000.000.000.000,
IP=000.000.000.000,IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,
IP=000.000.000.000,IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,
IP=000.000.000.000,IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,
IP=000.000.000.000,IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,
IP=000.000.000.000,IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,
IP=000.000.000.000,IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,
IP=000.000.000.000,IP=000.000.000.000,IP=000.000.000.000,ENDC,
NAME=,VIND=0,TRAP=NO,ACCESS=R,IP=000.000.000.000,
IP=000.000.000.000,IP=000.000.000.000,IP=000.000.000.000,ENDC,
END
```

where:

MIB	=	for future use only
GenTraps	=	switches on/off all traps
sysContact, sysName, and sysLocation	=	standard MIB II variables for system name, location, and contact personnel
NAME, VIND, TRAP (yes/no), ACCESS (read/write), and IP address	=	configurable SNMP community variables

2. Configure any of the following parameters:
   - GenTraps: set to "YES" if you want SNMP traps to be generated

     If you do not use SNMP on your network, set GenTraps to "NO".
   - Community Names
   - Access: "W" for read/write ("R" = read only)
   - IP Addresses
3. Return the revised data to the unit by sending a "set" command:

```
F100 config set snmp host:192.168.1.14
dir:temp
```

The unit responds:

```
Are you sure? (y/N)
```

If you answer "y", the unit responds:

```
Source file temp/snmp.conf bytes read: 1274
Dest File /config/snmp.conf bytes written: 1274
Configuration files transferred successfully!
```

and then resets.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter "y") to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

4.4.12 F100 LOCK – Remote Lockout

Use Remote Lockout to disable remote control capability and secure the unit from Telnet access. You can issue this command from Telnet or the serial port, or from the front panel. The default setting is "Unlocked". To once again activate remote access via Telnet, you *must* unlock the unit using the front panel (see Keypad Entry Guidelines and NET Port Network Parameters: First Time Configuration in Chapter 2).

To lock the unit from a remote location, send the following command:

F100 LOCK<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer "y" and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter "y") to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

If you are using Telnet when you issue this command and answer "y" and press Enter, the NTS executes the command by saying "Goodbye" and closing the Telnet session.

4.4.13 F100 L – Lock Display Request

Use Lock Display to view the lock setting state for remote Telnet access.

To view the lock setting for remote access, send the following command:

F100 L<Enter>

An example unit response:

```
UNIT_REMOTE_DISABLE_BIT = 0
```

This example shows that the unit is unlocked (0), so remote access is allowed.

Important Note:

The following commands related to sofware upgrades (F100 J, BH, BU, BUB, BF and K I L L) are not the normal commands used for uploading firmware. TrueTime provides these commands for flexibility in supporting special case situations. Normal firmware upgrades use an easy-to-use upgrade program provided with the firmware.

4.4.14 F100 J - Jumper

Use F100 PT to display the state of jumper JP5, which is reserved for future use. This function also displays the security flag bits and disable bits.

To display the state of jumper J5, send the following command:

F100 J<**Enter**>

An example unit response:

```
                    Jumper JP5 = 0
          Security flags = 0x00000000
                 FPC_SECURITY_BIT = 0
                 BURN_DISABLE_BIT = 0
            UNIT_REMOTE_DISABLE_BIT = 0
   PASSWORD_SETTING_DISABLE_BIT = 0
```

JP5 is located near the middle of the printed circuit board, beside the two flashing LEDs and the NetARM microprocessor.

4.4.15 F100 BH - Burn Host

Use Burn Host when upgrading software, to select the FTP host and the file to be transferred.

To select the FTP host and file for upgrading, send the following command:

F100 BH <FTP host IP address><**SP**>**<Upgrade file path>/<file name>**<**Enter**>

Use UNIX style forward slashes '/' in path and do not describe the drive (for example, 'C') in the path.

For example:

F100 BH 10.1.7.20 Lassen/Rel/REL20010518/nts200/192-9004v001.BIN

The unit responds:

```
Burn host is ready
```

This command can be disabled by the Burn Host Lock command, which denies serial and Telnet access. However, if you enter BootLoader mode, this command is always available.

4.4.16 F100 BU - Burn

Use Burn when upgrading software, to write the file selected with F100 BH to the flash memory. Flash memory is checked to ensure that the correct file is used.

To write the file to the flash, send the F100 BH command with the FTP host, file path and name, and then send the following command:

F100 BU<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer “y” and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

Unit example execution:

```
Burning Prog1
Burning file 182-9004v001.bin with size 688052 to
partition 1: sector :6
Sec: 6  re:  0
Sec: 7  re:  0
Sec: 8  re:  0
Sec: 9  re:  0
Sec: 10  re:  0
Sec: 11  re:  0
Sec: 12  re:  0
Sec: 13  re:  0
Sec: 14  re:  0
Sec: 15  re:  0
Sec: 16  re:  0
Flash successfully programmed CRC32 = 0x88841B88
```

4.4.17 F100 BUB - Burn BootLoader

Use Burn BootLoader when upgrading software, to write the BootLoader to flash memory.

To write the BootLoader to the flash, send the F100 BH command with the FTP host, file path and name, and then send the following command:

`F100 BUB`<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer “y” and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

unit example execution:

```
Burning Boot
Burning file 182-9003v001.BT with size 342860 to
partition 0: sector :0
Sec: 0  re:  0
Sec: 1  re:  0
Sec: 2  re:  0
Sec: 3  re:  0
Sec: 4  re:  0
Sec: 5  re:  0
Flash successfully programmed CRC32 = 0xE3E0ECAE
```

If more than six flash sectors are written during this process, you must rewrite both the bootloader sectors (0 to 5) and the program binary sectors (6 to 16).

4.4.18 F100 BF - Burn File System

Use Burn File System when upgrading software, to write a file system to the flash memory.

To write the file system to the flash, send the F100 BH command with the FTP host, file path and name, and then send the following command:

`F100 BF`<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer “y” and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

Unit example execution:

```
Burning file 182-9005v003.fs with size 524288
Sec: 20
Sec: 21
Sec: 22
Sec: 23
Sec: 24
Sec: 25
Sec: 26
Sec: 27
Sec: 28
```

4.4.19 F100 K I L L - Reboot

Use K I L L after upgrading software, to reboot the unit.

K I L L is a case-sensitive command. When entering this command, use all capital letters. You also must put spaces between each letter.

To reboot the unit, send the following command:

F100 K<SP>I<SP>L<SP>L<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer “y” and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

When using F100 K I L L via the Serial Port, pressing Y then Enter will begin the reboot, which will be logged on the terminal as shown below.

Unit example execution (Serial Port):

```
System Power On  Self Test Results:
Serial Loopback Test Passed.
...
Initialization Successfully Completed.
```

Press Enter, then you can log in again.

When using F100 K I L L via Telnet, pressing Y then Enter will begin the reboot, but will disconnect the Telnet session. Nothing will show on the terminal, and pressing Enter again will close the screen (if it hasn’t closed automatically already).

4.4.20 F100 BL - Burn Host Lock Request

Use Burn Host Lock to display whether or not software upgrades via serial or Telnet connections can be performed in the normal mode.

To display the burn host lock state, send the following command:

F100 BL<Enter>

An example unit response:

```
BURN_DISABLE_BIT = 0
```

If the lock is set to 1, upgrading is not possible via serial or Telnet connections in the normal mode (the burn host lock has been set). If the lock is set to 0, upgrading is possible (the burn host lock has been reset).

4.4.21 F100 BLS - Burn Host Lock Set

Use Burn Host Lock Set to prevent unauthorized upgrading of software via serial or Telnet connections.

To set the burn host lock, send the following command:

F100 BLS<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer “y” and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

Unit example execution:

```
BURN_DISABLE_BIT = 1
```

4.4.22 F100 BLR - Burn Host Lock Reset

Use Burn Host Lock Reset to reset the lock and allow software upgrades via serial and Telnet connections. You must be in bootloader mode to access this function.

To reset the burn host lock, send the following command:

F100 BLR<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer “y” and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter "y") to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

Unit example execution:

```
RESET BURN_DISABLE_BIT = 0
```

If you are in normal mode and you try to reset the burn host lock, you will get a friendly reminder:

```
Command Canceled
BURN_DISABLE_BIT = 1
Bootloader Mode Required
Reboot while holding SAVE key
```

4.4.23 F100 PRESETALL - Password Reset All

Use Password Reset All when you want to set passwords back to the factory defaults.

PRESETALL is a case-sensitive command. When entering this command, use all capital letters.

To reset all the passwords to factory defaults, send the following command:

F100 PRESETALL<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer "y" and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter "y") to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

Unit example execution:

```
Flash memory writing in progress:
Default user name and password set: 2
Default user name and password set: 1
```

4.4.24 F100 PN - Password System User Name Change

Use Password System User Name when changing the login user name.

To change the login user name, send the following command:

F100 PN<Enter>

The unit responds:

```
User Name Change for xyz123
Enter new user name:
```

When you enter a new user name, the unit responds with:

```
Confirm new user name:
```

Enter the same new user name again, to confirm the spelling.

If the same new user name has been entered twice, the NTS responds with:

```
User name change for xyz123 successfully changed
```

In this case, the new user name will be used for the next Telnet login. However, if the new user name is entered differently the second time, the NTS responds with:

```
ERROR: User names do NOT match. New user name rejected.
```

In this case, the old user name will be used for the next Telnet login.

4.4.25 F100 PR - Password Reset

Use Password Reset when changing the current login user name and password to their defaults.

To reset the passwords to factory defaults, send the following command:

F100 PR<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer “y” and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

Unit example execution:

```
Default user name and password set : 2
```

4.4.26 F100 PL - Password Lock Request

Use Password Lock to view the password changing lockout setting for Telnet sessions.

To display the password lockout state, send the following command:

F100 PL<Enter>

An example unit response:

```
PASSWORD_SETTING_DISABLE_BIT = 0
```

If the lock is set to 1, changing the password is not possible (the password lock has been set). If the lock is set to 0, changing the password is possible (the password lock has been reset).

4.4.27 F100 PLS - Password Lock Set

Use Password Lock Set to lockout setting of passwords via Telnet.

To inhibit password changes, send the following command:

F100 PLS<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer “y” and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

Unit example execution:

```
PASSWORD_SETTING_DISABLE_BIT = 1
```

4.4.28 F100 PLR - Password Lock Reset

Use Password Lock Reset to allow setting of passwords via Telnet.

To allow password changes, send the following command:

F100 PLR<Enter>

The unit responds:

```
Are you sure? (y/N)
```

If you answer “y” and press Enter, the unit executes the command.

As a safety feature, after sending this command, you have 10 seconds to respond affirmatively (enter the letter “y”) to the confirmation prompt, after which the unit executes the command and resets. Within that 10 second time period, any other response, including no response, results in the unit canceling the command.

Unit example execution:

```
PASSWORD_SETTING_DISABLE_BIT = 0
```

4.4.29 F100 PE LIST - Peer List Request

Use Peer List to view the NTP peers being polled every 64 seconds.

To display the peers, send the following command:

F100 PE LIST<Enter>

An example unit response:

```
Peer no: 001 127.127.001.000
Peer no: 002 206.254.000.020
```

4.4.30 F100 PE ADD - Peer Add

Use Peer Add to temporarily add an NTP peer node to be polled. After logging out, when you log back in the original peer settings will be active.

To add a peer, send the following command:

F100 PE ADD<IP Address><Enter>

For example:

F100 PE ADD 206.254.000.021<Enter>

4.4.31 F100 PE REM - Peer Remove

Use Peer Remove to temporarily remove an NTP peer node from the polling list. After logging out, when you log back in the original peer settings will be active.

To remove a peer, send the following command:

F100 PE REM<IP Address><Enter>

For example:

F100 PE REM 206.254.000.021<Enter>

4.4.32 F100 PI - PING

Use F100 PI to ping a remote host to see if it is reachable.

To ping a known host, send the following command:

F100 PI<IP Address><Enter>

For example:

F100 PI 206.254.000.021<Enter>

An example unit response:

```
PING: Remote Host Reachable.
```

4.4.33 F100 PT - Time

Use F100 PT to display UTC time in seconds.

To see UTC time in seconds, send the following command:

F100 PT<Enter>

An example unit response:

```
UTC: 990467862
```

4.5 Login/Logout

There are two levels of login: “operator” and “guest”.

5

NTS-Generated Messages

5.1 Error Messages

5.1.1 ERROR 01 VALUE OUT OF RANGE

Meaning: You have entered a valid command, with an invalid parameter value.

Recovery Action: Re-enter the command, using a valid parameter.

5.1.2 ERROR 02 SYNTAX

Meaning: You have entered a valid command with a minor syntax error. The NET Port network interface software has detected the error.

Recovery Action: Re-enter the command, using valid syntax.

5.1.3 ERROR: Invalid Command

Meaning: You have entered an invalid command.

Recovery Action: Consult the manual for the correct command and re-enter.

5.1.4 ERROR: Can't create netdevice <NAME>

Meaning: The NTS can not create the device needed to map the host to a drive.

Recovery Action: Restart the Unit. If this error message persists, contact TrueTime Technical Customer Service.

5.1.5 ERROR: Can't set host <NAME> ip <ADDRESS>

Meaning: You have incorrectly entered a parameter, or there is no room currently in the Host table for another IP Address.

Recovery Action: Verify correct parameter values. If correct, restart the NTS. If this error message persists, contact TrueTime Technical Customer Service.

5.1.6 ERROR: Action (get or set) is not specified

Meaning: You have omitted the “get” or “set” parameter from the F100 NTP Configuration command.

Recovery Action: Re-enter the command, specifying the desired action.

5.1.7 ERROR: Can’t open source file <NAME>

Meaning: The file containing the needed data is unavailable.

Recovery Action: Check file location and directory names to verify the path is accurate, then re-enter the command.

5.1.8 ERROR: Can’t open dest file <NAME>

Meaning: The destination file is unavailable.

Recovery Action: Check file location and directory names to verify the path is accurate, then re-enter the command.

5.1.9 ERROR: Can’t write file <NAME>

Meaning: Data from the source file cannot be copied to the destination file.

Recovery Action: Check file location and directory names to verify the path is accurate, then re-enter the command.

5.1.10 ERROR: Configuration failed.

Meaning: Your attempt to configure new parameters was unsuccessful.

Recovery Action: Verify parameter values, then re-enter the command.

5.1.11 ERROR: Configuration type is not specified

Meaning: You did not specify the file type.

Recovery Action: Re-enter the command, specifying SNMP and/or NTP.

5.2 LED System Status Alerts

5.2.1 Solid Red/Solid Orange

Meaning: Solid Red means there is no signal from the time source, or that a major alarm fault has been detected.

Solid Orange means that the NTS is in backup timing mode; synchronization has not been lost, but the unit is using NTP to synchronize time.

Recovery Action: Check your antenna installation for correct position, obvious hardware problems, or trouble with lines or wires. If you still need assistance, contact TrueTime at (707) 528-1230 or service@truetime.com.

5.3 Informational Messages

Messages in this section inform you of events and do not require any action on your part.

5.3.1 Deleted previously set IP host address

Meaning: Your last action deleted the previously set IP host address.

5.3.2 NOTICE: Cannot respond to command because Utility Port session has priority.

Meaning: A Utility Port session has started and takes precedence. Wait until it is over before logging in or expecting a response to an entered Telnet command.

5.3.3 Host <NAME> ip <ADDRESS> configured successfully!

Meaning: Host configuration was successful.

5.3.4 Source file <NAME> bytes read: <NUMBER>

Meaning: Source file was successfully read.

5.3.5 Dest file <NAME> bytes written: <NUMBER>
Configuration files transferred successfully!

Meaning: Information was successfully transferred to the destination file.

5.3.6 Restarting the Unit
Please wait…

Meaning: A command has just been executed that requires a soft restart of the NTS. The restart happens immediately after this message is sent.

5.3.7 DHCP is enabled

Meaning: You have just successfully entered the Enable DHCP command.

5.3.8 DHCP is disabled

Meaning: You have just successfully entered the Disable DHCP command.

5.3.9 OK

Meaning: Command accepted and processed as specified.

5.3.10 Goodbye.

Meaning: The NTS has just terminated a session. .

A

Network Time Protocol (NTP) V 3.0 Data Formats

This appendix describes the following two data formats:

- NTP V 3.0 per RFC-1305 (page A-2)
- SNTP V 3.0 per RFC-2030 (page A-5)

The NTS fully supports NTP version 4.0, (backwards compatible with NTP v.2, RFC-1119, and v.3, RFC-1305), and SNTP as per RFC 2030.

All RFCs are published with approval of the Internet Activities Board, found on the Internet by running any search engine and typing "RFC" in the search field (or “RFC-####” if you have the number). Two such search engines can be found at the following Internet addresses:

http://www.lycos.com/

http://www.altavista.com/

A.1 NTP V 3.0 Data Format per RFC-1305

A.1.1 NTP Data Packet

The layout of the NTP data packet information following the UDP header is shown below, and each element is described on the following pages:

Leap Indicator	Version Number	Mode	Stratum	Poll	Precision
Synchronizing Distance (Root Delay Version 3)					
Synchronizing Dispersion (Root Dispersion Version 3)					
Reference Clock Identifier					
Reference Timestamp					
Originate Timestamp					
Receive Timestamp					
Transmit Timestamp					
Authenticator					

Figure A-0 NTP Data Packet Information Layout

Leap Indicator

The leap indicator is a 2 bit code that signals an impending leap second to be added or subtracted in the last minute of the current day. Leap year codes and their corresponding meanings are shown in Table A-1 below:

Table A-1 Leap Year Codes

Bit 0	Bit 1	Meaning
0	0	Normal Operation
0	1	61 second last minute
1	0	59 second last minute
1	1	Clock not synchronized

The unsynchronized state is indicated by the NTS whenever the estimated synchronization error is greater than the root dispersion. Such conditions typically occur following turn-on, until synchronization with the external source has been achieved, and whenever the external synchronization input has been removed and the extrapolated time error has exceeded the value of the root dispersion.

Version Number

The version number is a three bit integer that specifies the NTP version. The NTS will copy this field from the client requesting packet and return it in this field if it is equal to either 2 or 3. NTP version 1.0 packets are not supported.

Mode

The mode is a three bit integer that determines the functions the NTS module will perform. TrueTime's NTS module operates in mode four or server mode. Mode four operation allows the module to synchronize hosts but will not allow the module to be synchronized by another host.

Stratum

The stratum is an eight bit integer providing the stratum level of the time source. TrueTime's NTS module operates in stratum 1, denoting a primary reference.

Poll Interval

The poll interval is a signed eight bit integer used as the exponent of two to yield in seconds the minimum interval between consecutive messages. For example, a poll interval value of six implies a minimum interval of 64 seconds. The NTS does not alter the setting of this field.

Precision

The precision is a signed eight bit integer used as the exponent of two to yield in seconds the precision of the local time source and any other hardware affecting the base level "jitter" of the time server. This field is set to approximate the time stamping resolution of the NTS, which is 10 µs. So the precision byte is set to –16, which is equivalent to a precision of 15.26 µs.

Synchronizing Distance (Root Delay Version 3)

The root delay is a signed 32 bit fixed point number representing the predicted round-trip delay in seconds to the primary synchronizing source. The fraction point is between bits 15 and 16. This value is set to 0 seconds in TrueTime's NTS module.

Synchronizing Dispersion (Root Dispersion Version 3)

The root dispersion is a signed 32 bit fixed point number representing the maximum error in seconds relative to the primary synchronizing source. This value is a function of the precision and the quality of the synchronization input option.

When the synchronization input option is GPS, then the NTS will self determine the accuracy. Once the accuracy has been determined, then the NTS sets the root dispersion equal to ten times the square root of the sum of the squares of the precision and the accuracy, except for the ACTS synchronization option, where the root dispersion is set equal to the accuracy.

Reference Clock Identifier

The reference clock identifier is a 32 bit code identifying the particular type of timing source. Strata 0 and 1 use a four-octet, left justified, zero-padded ASCII string. TrueTime's NTS module operates as Stratum 1 and uses this four-octet string based on the local time source input as shown in Table A-2 below. This setting is determined based on the NTS synchronization input option.

Table A-2 Local Time Source Input

Local Time Source Input	Reference Identifier String
GPS	"GPS"
NTP	"NTP"

Reference Timestamp

The reference timestamp is a 64 bit timestamp format representing the local time at the last update. TrueTime's NTS module's reference timestamp is the last time that a valid synchronization source signal was present.

Originate Timestamp

The originate timestamp is a 64 bit timestamp format representing the time that the request left the client host.

Receive Timestamp

The receive timestamp is a 64 bit timestamp format representing the time that the request arrived at the service host.

Transmit Timestamp

The transmit timestamp is a 64 bit timestamp format representing the time that the reply left the service host.

Authenticator

This is a 96-bit field containing the authenticator information as described in Appendix C of RFC-1305. This field is not implemented by the NTS.

A.2 SNTP V 3.0 Data Format per RFC-2030

When the NTS replies to requests from SNTP clients, the packet format is the same as the NTP packet format described above, with the following differences:

- Leap Indicator
  The NTS will set these 2 bits to either 0 (normal) or 3 (unsynchronized) only
- Version Number
  The NTS will copy this field from the client request packet and return it in this field.
- Reference Timestamp
  This field is set to the time that the reply left the NTS server host.
- Receive Timestamp
  This field is set to the time that the reply left the NTS server host.
- Transmit Timestamp
  This field is set to the time that the reply left the NTS server host.
- Authenticator
  This field is not used in SNTP.

B

MD5 Authentication and NTP Broadcast Mode

B.1 Introduction to MD5 Authentication Protocol

MD5 is a security protocol that can be used to authenticate NTP client-server communications, ensuring that a received NTP time packet is free from tampering. For example, if the server receives an NTP request packet with the wrong MD5 key (i.e., a key that hasn't been configured by the user in the NTS), then the server ignores the request. A similar mechanism exists on the client side. If the client makes a request with a specific key, and the response does not have the same key, then the client assumes the packet can not be trusted and discards it.

TrueTime's version of MD5 is compatible with all versions of NTP client software furnished by Dr. David Mills at the University of Delaware. MD5 was drafted into a standard by MIT Laboratory for Computer Science and RSA Data Security, Inc. MD5 authentication means the information within the NTP packet is guaranteed to be unaltered and from a user having privileged access. Unlike other cryptographic ciphers, MD5 does not hide the data within the packet. The MD5 authenticated NTP packet is still readable. This means MD5 is faster to generate than other cryptographic protocols, and as Dr. Mills notes, there is no reason to hide the actual time from anyone. Further, MD5 does not suffer from any export restrictions. You could think of MD5 as a very sophisticated NTP data checksum that is calculated over the data, socket address, and a private key of an NTP time packet. It is extremely difficult to reverse generate.

The MD5 cryptographic key identifier and cryptographic message digest are appended to the end of a normal NTP packet and the two pieces of information are referred to together as an MD5 signature. The key identifier is the first field in the signature, and it is a 32-bit integer in the range from 1 to 4294967295 (0xFFFFFFFF) – do not use zero as a key identifier. This number specifies an index into a table of many possible MD5 keys.

An MD5 key is an ASCII alpha/numeric character string that is from 1 to 32 characters in length. The key is most secure when all 32 characters are filled with numbers and letters chosen at random. The ASCII key string is combined with the NTP packet data and results in a secure message digest.

The MD5 message digest is 16 bytes in length and it follows the key identifier in the signature. A server authenticates the NTP packet from a client by first looking up the key by reference to the key identifier. It then generates the MD5 message digest based on the key and the NTP data and compares the resulting message digest to the client packet's MD5 message digest. If the two compare, a NTP reply packet is generated with a new MD5 signature. If the MD5 message digests do not agree, then the NTP client packet is ignored by the TrueTime server.

To use NTP Broadcast mode, you also need the following information:

- Maximum number of user definable MD5 keys in the "ntp.keys" file: **24**
- Maximum number of trusted keys that can be defined in an "ntp.conf" file: **20**
- Maximum number of keys that can be used in NTP broadcast mode: **20**
- Maximum text length of MD5 key value in "ntp.keys" file: **32 ASCII characters**

For more technical information on MD5, see the MD5 RFC-1321, NTP RFC-1305, and the release notes for NTP client software furnished by Dr. David Mills' web site located at the University of Delaware at:

http://www.eecis.udel.edu/~ntp
or

http://www.eecis.udel.edu/~ntp/software.html

All RFCs are published with approval of the Internet Activities Board, found on the Internet by running any search engine and typing "RFC" in the search field (or "RFC-####" if you have the number). Two such search engines can be found at the following Internet addresses:

http://www.lycos.com/

http://www.altavista.com/

B.2 NTP Broadcast Mode with MD5 Authentication

An NTP broadcast timeserver with an NTP broadcast time client can be used for NTP version 4 with authentication.

The MD5 authentication protocol is optionally available for NTP versions 3 and 4. When a packet is received by NTP, it checks the key identification number in the packet against the private key in the "ntp.keys" file, then calculates the MD5 digest number and compares this number to the one sent in the packet. If the digest numbers do not agree, then the packet is ignored. Thus, only servers with trusted MD5 keys may send time to a client. The keys are known to both the NTP client and server through separate key files, usually named "ntp.keys" in the "/etc" directory. The name of the file and its location are determined by the "–k" option when the NTP program is invoked.

In actual practice, for normal NTP client-to-server communications using explicit IP addresses with multiple servers, it is not necessary to use MD5. That is because the NTP client spends a great deal of time filtering out packets with incorrect time. Anyone attempting to send false time to a NTP client would be discarded. However, when broadcast time is used, then the client accepts the packet more readily and in this case can be fooled. The same is true if only one NTP server is used to synchronize an NTP client and a network attacker substitutes a false NTP server for the good one. Under these conditions, the NTP client has nothing to judge the time against and, if the false information is persistent, then the client will be forced to eventually reset its time. In this case it is worth the extra processing load to use MD5.

Setting up an NTP broadcast server and NTP client using MD5 authentication requires modifications to the "ntp.keys" file.

Editing MD5 keys is covered in Chapter 4 (see the sections starting on page 4-22). The following discussion covers the use of an NTP broadcast timeserver with an NTP broadcast time client for NTP version 4 without authentication.

B.3 NTP Broadcast Mode without Authentication

Authentication was configured *off* by default for NTP version 3, but is configured *on* by default for version 4. This means that NTP version 4 must use authentication, like MD5, for broadcast time to work. To have it otherwise, you must specifically turn authentication *off* in the "ntp.conf" file of the NTP time client.

The method outlined below should only be used when the LAN that the two NTP hosts are on is a secure network. Otherwise, it is all too easy for an NTP time imposter to broadcast the incorrect time to the NTP time client.

B.3.1 Configuration of NTP on the Timeserver

For the NTP timeserver, authentication may be on or off - it does not matter. As an example, here is a sample "ntp.conf" file.

```
server      192.168.1.49
server      206.54.0.20
server      206.54.0.21
broadcast   192.168.1.255
```

This file is stored on the TrueTime timeserver in its Flash disk drive in the "/etc" directory.

The critical line is: `broadcast 192.168.1.255.`

- This line turns on the periodic broadcast of NTP time packets to the local LAN. This IP address (the first three octets: 192.168.1) is a network address.

  The LAN portion of the address, the last octet in this case, is set to all ones. You may use all zeros for most LANs as the LAN address, instead of all ones. This address allows NTP time packets to be received by all hosts on the local LAN including the NTP time client. Ask your system administrator what your LAN broadcast address is for your particular network and substitute it for the address in this example.

B.3.2 Configuration of NTP on the Time Client

Authentication status is critical on the time client. If MD5 is not used, authentication *must* be *off* for broadcast mode to work. Here is a sample "ntp.conf" file used in the time client, plus a sample command line of the NTP program invocation:

```
server      192.168.1.49
server      206.54.0.20
server      206.54.0.21
disable auth
```

This file is stored in the "/etc" directory on the time client or the same directory that "ntp.conf" is stored if your directory is different from the standard NTP default directory. The critical line is: `disable auth`.

- The line `disable auth` turns off system authentication and tells the system to not use authentication for received NTP time broadcast packets.

When you invoke the NTP client at the command line, use the following options:

- `-b`
  to turn on broadcast packet reception
- `-d`
  to turn on debug mode at a sufficient level to verify that broadcast packets are indeed being used:
  `ntpd -d -d -d -b`

Once you have completed debugging your system, you can prevent incoming messages from appearing on the command line by turning off the debug option flags.

B.4 Polling

The designated server contacts every server each time it polls for time. Out of the responses, it picks the best one and uses that as its primary synchronization source. The "best" one is determined based on a combination of stratum (lowest is best), network delays (closest is best), advertised precision (smallest is best), plus other criteria that is not detailed. If the "best" server goes away, after consecutive polling periods with no response from that server the unit will choose one of the remaining servers to be the synchronizing source.

In a client/server mode the server (or any NTP client) adjusts the poll interval to maintain timing between 1 - 10 milliseconds if possible. The interval starts out at the default value of every 64 seconds, but then lengthens based on the size of the calculated offsets. The server also starts estimating the average drift of the internal oscillator, and uses this information to refine its polling period. The typical polling period ends up being about 5 to 8 minutes. This polling period is self-adjusting and can not be adjusted externally.

C

TIME and DAYTIME Protocols

C.1 TIME Protocol as per RFC-868

TIME protocol provides a site-independent, machine readable date and time. The TIME service sends back to the originating source the UTC time in seconds since midnight on January 1, 1900.

This protocol may be used either above the Transmission Control Protocol (TCP) or above the User Datagram Protocol (UDP).

When used via UDP, the TIME service works as follows:

Server:Listen on port 37 (45 octal).

Client:Send an empty datagram to port 37.

Server:Send a datagram containing the UTC time as a 32 bit binary number.

Client:Receive the TIME datagram.

The server listens for a datagram on port 37. When a datagram arrives, the server returns a datagram containing the 32-bit time value. If the server is unable to determine the time at its site, it should discard the arriving datagram and make no reply.

C.1.1 The Time Protocol Format

The time is the number of seconds since 00:00 (midnight) 1 January 1900 UTC, such that the time 1 is 12:00:01 AM on January 1, 1900 UTC; this base will serve until the year 2036.

C.2 DAYTIME Protocol as per RFC-867

DAYTIME protocol pertains to a daytime service, a useful debugging and measurement tool. A daytime service simply sends the current date and time as a character string without regard to the input.

C.2.1 TCP Based Daytime Service

This daytime service is defined as a connection based application on TCP. A server listens for TCP connections on TCP port 13. Once a connection is established, the current date and time is sent out the connection as a ASCII character string (and any data received is thrown away). The service closes the connection after sending the quote.

C 2.2 UDP Based Daytime Service

This daytime service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 13. When a datagram is received, an answering datagram is sent containing the current date and time as a ASCII character string (the data in the received datagram is ignored).

C 2.3 DAYTIME String Format

The string format for the DAYTIME Protocol conforms to the Unix workstation time expression, except the time is in UTC rather than local time. The syntax is as follows:

```
DDD, MMM, XX, YYYY, HH:MM:SS-UTC
```

where

DDD	=	the day: “Sun”, “Mon”, “Tue”, “Wed”, “Thus”, “Fri”, “Sat”
MMM	=	the month: “Jan”, “Feb”, “Mar”, “Apr”, “May”, “Jun”, “Jul”, “Aug”, “Sep”, “Oct”, “Nov”, “Dec”
XX	=	day of the month
HH	=	hour (24 hour format) of that day
MM	=	minutes of that hour
SS	=	seconds of that minute

D

SNMP – Simple Network Management Protocol

D.1 About SNMP

SNMP management software allows a network user to remotely monitor and configure an IP host that supports an SNMP agent. An SNMP agent is protected from unauthorized use through a security scheme. The TrueTime NTS supports a SNMP version 1 agent with the MIB II and Enterprise MIB databases.

The material in this section assumes you already have an understanding of SNMP. If that is not the case, we recommend “SNMP, SNMPv2 and CMIP” written by William Stallings and published by Addison-Wesley Publishing Company. This book is considered by the community to be the definitive introduction to SNMP. Another good reference is “How To Manage Your Network Using SNMP,” by Marshal T. Rose and Keith McClogurie. For more technical references, see RFC-1157 (the definition of SNMPv1), RFC-1213 (the definition of MIB II) and RFC-1354 (the IP Forwarding table addition to MIB II). All RFCs are published with approval of the Internet Activities Board, found on the Internet by running any search engine and typing "RFC" in the search field (or “RFC-####” if you have the number). Two such search engines can be found at the following Internet addresses:

http://www.lycos.com/

http://www.altavista.com/

Two sites in particular that have basic information on SNMP are:

The Simple Web: http://snmp.cs.utwente.nl/

Basic SNMP Information: http://www.skyweb.net/~parsons/snmp-links.html

D.2 TrueTime SNMP Configuration

SNMP offers a security authentication scheme that is based on a common password shared by the management station and a group of agents. A group of hosts are known as a community. Any management station or agent can be a member of any combination of communities. Typically a manager will need to change the SNMP community information from TrueTime's SNMP agent factory defaults for security purposes. However, the factory default SNMP community settings are chosen to make the TrueTime SNMP immediately usable. TrueTime's SNMP agent recognizes up to five separate SNMP communities. These communities are configured through the serial or Telnet interface using the F100 NTP command, where the "menus" referred to in this section appear. Each community has several configurable parameters that are defined in Table D-1.

Table D-1: SNMP Community Configurable Parameters

Key Word	Definition
Community Name	The name of this community. The name is limited to up to 32 ASCII letters, numbers or punctuation letters. This is the name that a management SNMP PDU (packet) specifies. If the community name of an incoming PDU does not match any of the five community names, the packet is ignored and an optional authentication trap message can be generated. See traps below. An empty string field disables the community name.
Trusted IP Address	If the Use Trusted IP flag is set to yes, then this is the table of IP host addresses that this community recognizes as valid SNMP management hosts. Even if the community name of an incoming PDU matches this community, the source IP address must match one of the IP addresses in this table, or the packet is ignored and an optional authentication error trap message is issued. Setting an IP address to all zeros turns off that IP address entry. In addition, this table also serves as the list of hosts that SNMP trap messages are sent to – regardless of the state of the Use Trusted IP flag.
Use Trusted IP	If this flag is set to yes, then the Trusted IP Address table is used in addition to the Community Name for authentication of incoming PDUs).
R/W Access	For a particular community, the SNMP variables are set to read only, or normal SNMP access. This allows the manager to have a public known community from which anyone may read the SNMP data base and a separate private community that has full normal read and write access to the SNMP database. ***Note:*** SNMP MIB II does not define all variables to be writeable. SNMP variables defined by RFC-1213 as read-only remain read-only, regardless of the state of this R/W Access flag.
Trap Enable	When this flag is set to yes, trap messages are issued for this community. ***Note:*** This enables/disables all traps (both coldstart and authentication).
Trap Port	A trap port other than the normal SNMP trap port of 162 may be specified. ***Note:*** This address must be chosen carefully, or conflicts with other protocols may occur.
Save settings	When any setting is changed, this becomes visible and answering yes immediately saves the changes to TrueTime's SNMP. Answering No will negate the changes.

Table D-2 and Table D-3 define SNMP configurable parameters that are applied globally to all SNMP communities (this menu appears after the last community menu), and the TrueTime SNMP factory default settings.

Table D-2: SNMP Community Global Parameters

KeyWord	Definition
SNMP Global Enable Traps	When set to yes, all authentication failure traps are disabled. This flag overrides the Trap Enable flag set for each community and directly sets the value of the SNMP variable snmpEnableAuthenTraps.0. ***Note:*** The state of this flag has no effect on the issue of coldstart trap messages.
Return To Main Menu	This leads back to the main SNMP function window.
Save settings	When SNMP Global Enable Traps is changed, this becomes visible and answering yes immediately saves the change to TrueTime's SNMP. Answering No negates the change.

Table D-3: TrueTime SNMP Default Settings

Key Word	Definition
Community 1	
Community Name	Public
Trusted IP Address	0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0
Use Trusted IP	No
R/W Access	read/only
Trap Enable	No
Trap Port	162
Community 2	
Community Name	System
Trusted IP Address	0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0
Use Trusted IP	No
R/W Access	Normal
Trap Enable	No
Trap Port	162
Community 3 to 5	
Community Name	
Trusted IP Address	0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0
Use Trusted IP	No
R/W Access	read/only
Trap Enable	No
Trap Port	162
SNMP Global Enable Traps	Yes

The factory default settings are summarized as follows: community one is called *public* and is set to read-only access for the SNMP MIB; community two is named *system* and it has normal access to the SNMP database; all other communities are disabled. All traps are disabled. Many SNMP management utilities are written with these default assumptions and thus the TrueTime SNMP is immediately usable without configuration.

D.3 Serial or Telnet Configuration

Use Serial or Telnet Function F100 CONFIG to obtain information about the current SNMP/NTP configuration, or to change the IP addresses, traps, read/write access, or community names and parameters. For details, see "Configuration of SNMP Parameters Using FTP" on page 4-24. Although this option is available, it is much faster and easier to configure SNMP parameters over the Internet. For details, see "Remote SNMP Configuration" on page 3-6.

D.4 TrueTime SNMP Enterprise MIB

Introduction

A Management Information Base (MIB) is a database of managed objects that have a hierarchical structure. There are common or vendor-specific managed objects. The Internet community has over 1,000 objects registered. The objects themselves are representations of real physical network properties or information.

Using a TCP/IP network and TrueTime's SNMP Enterprise MIB, you can remotely obtain information on the health and status of the NTP application and the primary time synchronization source using the SNMP version 1 protocol. The Enterprise MIB database has five variable groups: the Trap Message Group, the Network Time Protocol Group, the Network Time Server Control Group, the GPS Group, and the ACTS Group. Presently, the control group is preliminary and is not implemented in the current version of software.

Traps are sent on Change of Status (COS). There are three types of traps: NTP Status, GPS Status, and GPS Antenna Status. All of them report failures, as well as the return to active status. The settings are as follows:

- NTP Status: NTP Client Mode*
NTP Unlocked
NTP Locked
- GPS Status: GPS Locked
GPS Unlocked
- GPS Antenna Status: GPS Antenna Fault
GPS Antenna OK

*In NTP Client Mode, NTP is using another NTP server as its timing reference, instead of GPS.

The trap message group holds the ASCII string data to send whenever an SNMP trap message is transmitted. The NTS agent sends SNMP trap messages to SNMP management hosts notifying them of some critical event at the NTS agent. The NTS issues three types of trap messages. The first type is a cold start trap message indicating when the box boots or re-initializes. The second type of trap message is issued when the NTS estimated time error has exceeded the minimum time accuracy threshold. The third trap message is issued when a packet received by the NTS agent fails SNMP authentication. The second feature notifies a network administrator immediately if the time server lost its ability to tell accurate time.

The NTP Enterprise Group furnishes information on the Network Time Protocol. This group provides packet information for the number of received, rejected, and transmitted NTP packets exchanged between the UDP transport and the NTP application layers. Packets are rejected when they are malformed or the MD5 encryption authentication failed. In addition, time quality can be assessed by looking at the current estimated time error and comparing it with the time accuracy threshold. Finally, all of the NTP control information transmitted by the NTS in an NTP packet is available in this enterprise group. One important variable in this group is ntpSysLeap because it is the clearest indication if the NTS is telling correct time.

When GPS is used as the time synchronization source, the GPS Enterprise MIB Group provides detailed information about the satellites used by the NTS time server. Complete GPS satellite information exists on the number of satellites tracked and used for timing purposes, their signal strengths, the tracking mode, altitude, longitude, and latitude of the GPS antenna. This information allows you to properly set up the GPS antenna and to use the unit for time information.

When ACTS is used as the time synchronization source, the ACTS Enterprise MIB Group provides detailed information on the ACTS dial-up modem time service. Complete information on the number and success of the ACTS phone calls as well as a detailed break down of the various possible modem and line failures that can occur. This information allows you to fine tune calling frequency with the desired time accuracy and assess the telephone line quality of the connection to the ACTS service.

Obtaining the enterprise MIB information requires you to have an SNMP management program running on your computer.

Variable Definitions

This section contains a complete and formal definition of TrueTime's SNMP enterprise MIB group, including all the variables in TrueTime's Enterprise MIB, along with the MIB OID address and data types.

An electronic form of this file was included with this manual. If the disk has been misplaced or corrupted, a copy can be obtained from TrueTime's web site (www.truetime.com). Select **Products and Literature>Reference Material** to get there. The file's name is "TrueTime.MIB", and should compile for virtually any SNMP management software. It has been verified to work for Sun's Solaris X-SNMP and Hewlett Packard's OpenView management software packages.

TrueTime DEFINITIONS ::= BEGIN

IMPORTS

OBJECT-TYPE FROM SNMPv2-SMI
Counter FROM RFC1155-SMI
DisplayString FROM SNMPv2-TC
TRAP-TYPE FROM RFC-1215;

--iso OBJECT IDENTIFIER ::= { 1 }
org OBJECT IDENTIFIER ::= { iso 3 }
dod OBJECT IDENTIFIER ::= { org 6 }
internet OBJECT IDENTIFIER ::= { dod 1 }
private OBJECT IDENTIFIER ::= { internet 4 }
enterprises OBJECT IDENTIFIER ::= { private 1 }
trueTimeEnt OBJECT IDENTIFIER ::= { enterprises 1896 }

TrueTime MODULE-IDENTITY
LAST-UPDATED"9910250000Z"
ORGANIZATION"TRUETIME INC."
CONTACT-INFO"Technical Support"
DESCRIPTION
" This is the TrueTime enterprise MIB"
::= { trueTimeEnt 1 }
trapMsg OBJECT IDENTIFIER ::= { trueTimeEnt 2 }
ntp OBJECT IDENTIFIER ::= { trueTimeEnt 3 }
ntsControl OBJECT IDENTIFIER ::= { trueTimeEnt 4 }
gps OBJECT IDENTIFIER ::= { trueTimeEnt 5 }
acts OBJECT IDENTIFIER ::= { trueTimeEnt 6 }

trapMsgColdStart OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is an ASCII string sent to UDP port 162 (or user defined) when the TrueTime time server reinitializes. The message is Cold Start Trap PDU from: ###.###.###.###. Where ###.###.###.### is the dotted decimal notation of the IP address of the booting unit. ::= { trapMsg 1 }

trapMsgNtpAlarm OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is an ASCII-string sent to the UDP-trap port(162 or user defined) when the TrueTime time server's detects change of the NTP-status. This could be due to a line breakage in the timing source, loss of GPS satellites, etc. The message is 'NTP Status aaaaaaaa', where aaaaaaaaa can be NTP UNLOCKED,NTP client mode or NTP LOCKED. ::= { trapMsg 2 }

trapMsgSnmpAuthFail OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is an ASCII string sent to UDP port 162 (or user defined) when the TrueTime time server determines the SNMP authentication for a SNMP PDU is incorrect. The message is 'SNMP Authentication Failure Trap PDU from: ###.###.###.###', where ###.###.###.### is the dotteddecimal notation of the IP address of the unit attempting the invalid access. ::= { trapMsg 3 }

trapMsgGpsAntennaFault OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is an ASCII string sent to UDP trap port(162 or user defined) when the TrueTime time server's GPS detects change in the antenna status. The status can be OK or FAULT. ::= { trapMsg 4 }

trapMsgGpsUnlocked OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is an ASCII string sent to UDP trap port (162 or user defined) when the TrueTime time server's GPS detects change of the GPS status. The status can be is unlocked. ::= { trapMsg 5 }

ntpInPkts OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Total number of NTP packets delivered to the NTP application layer from the transport layer. ::= { ntp 1 }

ntpOutPkts OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Total number of NTP packets passed from the NTP application layer to the transport layer." ::= { ntp 2 }

ntpInErrors OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Total number of NTP packets reject for any reason by NTP application layer. ::= { ntp 3 }

ntpAuthFail OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Total number of authentication failures. This is a subset of ntpInErrors. ::= { ntp 4 }

ntpDesiredAcc OBJECT-TYPE
SYNTAX INTEGER (0..2147483647)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: The desired (worst case time) accuracy in microseconds that the time server will attempt to steer to. This variable is related to ntpEstError. Should ntpEstError be greater than ntpDesiredAcc, the NTP alarm condition will be set (ntpSysLeap will be equal to 3). Note: outgoing NTP packets will have their leap indicator field set to ntpSysLeap. ::= { ntp 5 }

ntpEstErr OBJECT-TYPE
SYNTAX INTEGER (0..2147483647)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: The current estimated (time) error in microseconds of the time server. This variable is related to ntpEstError. Usually, this value is small and constant for a given type of time server. However, when primary synchronization is lost, this value will slowly increase with time as the time server's oscillator flywheels away from true time. Should ntpEstError be greater than ntpDesiredAcc, the NTP alarm condition will be set ntpSysLeap will be equal to 3). Note: a primary time server's outgoing NTP packets will have its leap indicator field set to ntpSysLeap. ::= { ntp 6 }

ntpSysLeap OBJECT-TYPE
SYNTAX INTEGER
{noLeapWarningAndTimeIsSynchronized (0),
lastMinuteHas61SecondsAndTimeIsSynchronized (1),
lastMinuteHas59SecondsAndTimeIsSynchronized (2),
alarmConditionAndLossOfTimeSynchronization (3)}
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is a status code indicating normal operation, a leap second to be inserted in the last minute of the current day, a leap second to be deleted in the last second of the day or an alarm condition indicating the loss of timing synchronization. Note: a primary time server's outgoing NTP packet will have its leap indicator field set to ntpSysLeap. ::= { ntp 7 }

ntpSysHostMode OBJECT-TYPE
SYNTAX INTEGER
{hostModeIsReserved0 (0),
hostModeIsSymmetricActive (1),
hostModeIsSymmetricPassive (2),
hostModeIsClient (3),
hostModeIsServer (4),
hostModeIsBroadcast (5),
hostModeIsReserved6 (6),
hostModeIsReserved7 (7) }
MAX-ACCESS read-only
STATUS current
DESCRIPTION: The value of this variable indicates the mode that the host is operating in. Note: this is the value of the time server's outgoing NTP packet mode field.
::= { ntp 8 }

ntpSysStratum OBJECT-TYPE
SYNTAX INTEGER (1..255)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is an integer that ranges from 1 to 255 indicating the stratum level of the local clock. Note: a primary time server sets outgoing NTP packets stratum field and ntpSysStratum to 1. ::= { ntp 9 }

ntpSysPoll OBJECT-TYPE
SYNTAX INTEGER (6..10)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: When the time server is in NTP broadcast mode, this is an integer indicating the maximum interval between successive NTP messages, in seconds to the nearest power of two. For example a value of 6 means 2^6 or 64 seconds. Note: a primary time server's outgoing NTP packet will have its poll field set to ntpSysPoll. Note: this field is equal to 0 when not in NTP broadcast mode. Note, unless this is a time server initiated NTP packet the value of the poll equals the value set in the in coming packet.
::= { ntp 10 }

ntpSysPrecision OBJECT-TYPE
SYNTAX INTEGER (-127..127)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is an integer indicating the ultimate precision of the synchronizing clock, in seconds to the nearest power of two. Note: a primary time server's outgoing NTP packet will have its precision field set to ntpSysPrecision. ::= { ntp 11 }

ntpSysRootDelay OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is a raw 32 bit number representing a signed fixed point 32-bit number indicating the total round-trip delay to the primary synchronization clock source in seconds with the fraction point between bits 15 and 16. Note that this variable can take on both positive and negative values, depending on clock precision and skew. Note: a primary time server's outgoing NTP packet will have its root delay field set to ntpSysRootDelay. ::= { ntp 12 }

ntpSysRootDisp OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is a raw 32 bit number representing a signed 32-bit fixed-point number indicating the maximum error relative to the primary reference source, in seconds with fraction point between bits 15 and 16. Only positive values greater than zero are possible. Note: a primary time server's outgoing NTP packet will have its root dispersion field set to ntpSysRootDisp. ::= { ntp 13 }

ntpSysRefClockIdent OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..4))
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is a four byte ASCII string identifying the particular reference clock. In the case of stratum 0 (unspecified) or stratum 1 (primary reference), this is a four-octet, left-justified, zero-padded ASCII string. While not enumerated as part of the NTP specification, the following are suggested ASCII identifiers:

Stratum	Code	Meaning
0	DCN	DCN routing protocol
0	NIST	NIST public modem
0	TSP	TSP time protocol
0	DTS	Digital Time Service
1	ATOM	Atomic clock (calibrated)
1	VLF	VLF radio (OMEGA, etc.)
1	callsign	Generic radio
1	LORC	LORAN-C radionavigation
1	GOES	GOES UHF environment satellite
1	GPS	GPS satellite positioning
1	ACTS	ACTS telephone modem dial-up
1	IRIG	Inter-Range Instrumentation Group signal

Note: for TrueTime time servers only GPS, ACTS and IRIG are presently used. Further, a primary time server's outgoing NTP packet will have its reference identifier field set to ntpSysRefClockIdent. ::= { ntp 14 }

ntpControlInput OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-write
STATUS current
DESCRIPTION: This variable emulates TrueTime's serial function command strings. The same commands issued to the serial port can be sent to this string. Use this variable for SNMP sets of functions strings. Note, setting this variable clears ntpControlOutput to the null string. See ntpControlOutput below. ::= { ntsControl 1 }

ntpControlOutput OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This variable emulates TrueTime's serial function command strings. The same commands issued to the serial port can be sent to this string. This variable holds the output result string from the last setting of the above ntpControlInput variable. Use this variable for SNMP gets of function strings. See ntpControlInpuut above.
::= { ntsControl 2 }

gpsGroupValid OBJECT-TYPE
SYNTAX INTEGER
{gpsGroupIsInvalid (0),
gpsGroupIsValid (1)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: A test flag indicating if data contained in this SNMP GPS group is valid or not. This flag equals 1 when GPS is used as the time synchronization source and 0 for all other sources. ::= { gps 1 }

gpsNumTrackSats OBJECT-TYPE
SYNTAX INTEGER (0..8)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: The number of GPS satellites tracked. ::= { gps 2 }

gpsNumCurrentSats OBJECT-TYPE
SYNTAX INTEGER (0..8)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Current number of GPS satellites used in position and time fix calculations. The number of satellites available depends on how long the time server has been up, the time of day and the total amount of clear sky as seen from the GPS antenna. Because of the high frequency of GPS radio signals, GPS antennas must have unobstructed line of sight from the antenna to the satellite to receive data. ::= { gps 3 }

gpsSatTrackMode OBJECT-TYPE
SYNTAX INTEGER
{automaticMode (0),
timeMode (1),
surveyStaticMode (2),
surveyDynamicMode (3)}
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Mode of operation for satellite tracking. The NTS-200 uses only Survey Static Mode. See the user's manual for the NTS-100 series for a complete description of the modes it uses. Generally, modes 0 and 1 are used for time applications. Mode 2 is useful for more accurate position information when the unit is stationary, or slowly moving and mode 3 is for accurate position information when the unit is moving quickly. ::= { gps 4 }

gpsSatMaxSigStrength OBJECT-TYPE
SYNTAX INTEGER (0..30)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Strongest signal strength of all tracking satellites seen by the GPS receiver. The signal strength of the NTS-100 series~ is in linear units. The minimum is 4. The signal strength of the NTS-200 is in DBs. The minimum is -10. ::= { gps 5 }

gpsAltitude OBJECT-TYPE
SYNTAX INTEGER (-2147483647..2147483647)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Altitude of the GPS antenna in centimeters above, or below the WGS-84 reference ellipsoid. The reference ellipsoid is a rotated ellipse that is centered on the Earth's center of mass. The surface of the ellipsoid is not necessarily the same as sea level. The ellipsoid surface may be as much as 100 meters different from actual sea level.
::= { gps 6 }

gpsLongitude OBJECT-TYPE
SYNTAX INTEGER (-2147483647..2147483647)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Longitude location of GPS antenna where: +2147483647 is maximum east longitude, -2147483647 is maximum west longitude and 0 is Greenwich England. To calculate the longitude in radians use the following formula (gpsLongitude * PI) / ((2^31)-1) = longitude in radians. For degrees: (gpsLongitude * 180) / ((2^31)-1) = longitude in degrees. Note: longitude varies from -PI to +PI in radians and -180 to +180 in degrees. ::= { gps 7 }

gpsLatitude OBJECT-TYPE
SYNTAX INTEGER (-2147483647..2147483647)
MAX-ACCESS read-only
STATUS current
:DESCRIPTION Latitude location of GPS antenna where: +2147483647 is the North Pole, -2147483647 is the South Pole and 0 is the equator. To calculate the latitude in radians use the following formula gpsLatitude * PI) / (2*((2^31)-1)) = longitude in radians. For degrees: (gpsLatitude * 90) / ((2^31)-1) = latitude in degrees. Note: latitude varies from -PI/2 to +PI/2 in radians and -90 to +90 in degrees.
::= { gps 8 }

actsGroupValid OBJECT-TYPE
SYNTAX INTEGER
{actsGroupIsInvalid (0),
actsGroupIsValid (1)}
MAX-ACCESS read-only
STATUS current
DESCRIPTION: A test flag indicating if data contained in this SNMP ACTS group is valid or not. This flag equals 1 when ACTS is used as the time synchronization source and 0 for all other sources. ::= { acts 1 }

actsBaudRate OBJECT-TYPE
SYNTAX INTEGER
{baud300 (300),
baud1200 (1200)}
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Indicates the baud rate setting for the ACTS modem. The ACTS dial-up service accepts 300 or 1200 baud. Note: this is a rare case where faster is not better and 300 baud yields the best time accuracy. ::= { acts 2 }

actsFailRedial OBJECT-TYPE
SYNTAX INTEGER (0..9999)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: When the dial-up session fails to connect this is the time in seconds to wait to try again.
::= { acts 3 }

actsMaxCallPeriod OBJECT-TYPE
SYNTAX INTEGER (0..999)
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is the maximum time in hours the ACTS unit will wait between successful calls to the ACTS service. ::= { acts 4 }

actsPhoneNum OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..25))
MAX-ACCESS read-only
STATUS current
DESCRIPTION: This is the phone number of the ACTS dial-up service, including any prefixes needed to reach an outside line or international dialing. Prefixes are separated by a comma from the main phone number. ::= { acts 5 }

actsNumberOfCalls OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Number of times the time server has called the ACTS dial-up service - weather the call was successful or not. ::= { acts 6 }

actsGoodCalls OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Number of times the time server called the ACTS dial-up service and successfully received the time. ::= { acts 7 }

actsBadCalls OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Number of times the time server called the ACTS dial-up service and something was not right. This variable is the sum total of all other ACTS failure types. ::= { acts 8 }

actsFailedInit OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Time server's internal modem failed to initialize. If this is excessive, it may indicate a time server hardware failure. ::= { acts 9 }

actsNoDialTone OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Time server's internal modem found no dial tone. This may be caused by a broken phone line to the time server. ::= { acts 10 }

actsNoCarrier OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Time server's internal modem found no carrier. No modem was found at the other end and maybe the phone number for ACTS is wrong. ::= { acts 11 }

actsBusyLine OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: Time server's internal modem found ACTS line busy. ::= { acts 12 }

actsNoAnswer OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: The remote ACTS mode did not answer the call. ::= { acts 13 }

actsBadReply OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: The syntax of the reply from remote modem was incorrect, possibly due to line noise.
::= { acts 14 }

actsNoOnTimeMark OBJECT-TYPE
SYNTAX Counter
MAX-ACCESS read-only
STATUS current
DESCRIPTION: The reply from remote modem had no on time mark, possibly due to line noise.
::= { acts 15 }

END

E

Non-Standard Features

This appendix contains information on optional features that may have been added to your device at the factory. For a standard device, it is normal for this appendix to be empty.

Index

Numerics

10Base-T/100Base-T *1-8*, *2-5*, *4-12*
    Control Command (F100 BASET) *4-12*
-48 VDC Model
    Cabling *2-4*
    Power Specifications *1-5*

A

AC Model
    Cabling *2-4*
    Power Specifications *1-5*
Access *1-2*, *3-7*, *D-2*
    HTTP *3-1*
    Internet *3-7—3-9*
    Remote Control Lockout (F100 LOCK) *2-11*
    Remote Lockout (F100 LOCK) *4-26*
    Serial *3-9—3-14*
    Web *3-1*
Accuracy *1-6*
Acquisition *2-3*
ACT (Connection Speed Indicator LED) *1-7*
Administrator *2-14*
Antenna *1-3—1-4*, *2-2—2-3*, *2-5*, *2-7*
    Feed Circuit Status (F72) *4-10*
    Installation *2-1*
    Mast Mounting *2-3*
Applications, List of Supported *1-8*
Authentication *D-2*
    Broadcast Mode with *4-22—4-23*, *B-3*
    Broadcast Mode without *B-4—B-5*
Auto-Configure *4-13*
Automatic Time Out
    For Display Security Feature *2-12*

B

Backward Compatibility *4-7*
Bad Satellite *4-8*
Broadcast Mode
    Editing MD5 Keys *4-22—4-23*
    with Authentication *4-22—4-23*, *B-3*
    without Authentication *B-4—B-5*
Browser *3-2*
    Addresses *A-1*, *B-2*, *D-1*
    See also, Web

C

Cabling *2-4—2-5*
Change User Password (F100 P) *4-16*
Chassis *1-3*, *2-5*
Cold Boot *2-6*
Commands
    and Responses, Serial/Telnet
        Common Elements *4-5*
    Serial/Telnet
        Format *4-1*
        List *4-3—4-4*
        Semicolon used as replacement *4-2*
Community *D-2*
Compatibility *4-7*
Configuration *D-2*
    Commands (F36 or F100) *4-7*
    NET Port
        Initial *2-13—2-14*
        Single Entry (F100) *4-11*
        Using Serial/Telnet Commands *4-11*
        Using the Internet *3-3*, *3-6*
    NTP *4-21*
        Using FTP *4-21—4-25*
        Using the Internet *3-4*
    Remote Control Lockout (F100 LOCK) *2-11*, *4-26*
    SNMP
        Using FTP *4-24*
        Using the Internet *3-6*
Configuration Control Login Web Page *3-2*
Connection *1-2*, *2-2*, *3-1*, *3-7*, *3-10*, *3-15*, *4-12*
Connector *1-2*, *1-8*, *2-2*, *2-4*, *3-9*
Control Session *3-7*
Conventions *1-1*
Current Satellite *4-8*
Cursor *2-9*, *2-13*

D

Data Packet
    NTP *A-2*
Data Rates *1-8*, *3-9*
Datagram *C-1*
Date *1-2*
DAYTIME Protocol *1-6*, *C-2*
Default Gateway (F100 G) *4-15*
Delay *A-2—A-3*
DHCP *1-6*, *1-8*, *5-4*
    Command (F100 DHCP) *4-13*
    Start-Up Display *2-10*
Display *1-7*, *3-3*
    Default *2-7*
    Power-Up Sequence *2-6—2-8*

Display Security *2-10—2-12*
Automatic Time Out *2-12*
Logout *2-12*
Distance *A-2*
Down Converter *1-3*, *2-3*
DTR *3-9*

E

Enabled Satellite *4-8*
Enterprise MIB *2-14*, *D-1*, *D-4*
Environmental Specifications *1-4*
Error Messages *5-1*
Ethernet *1-2*, *1-8*, *2-2*, *3-1*, *4-13*
10Base-T/100Base-T *4-12*
Ethernet Address (F100 EA) *4-14*

F

F03 *4-6*
F100 *4-11*
F100 BASET *4-12*
F100 BF *4-29*
F100 BH *4-27*
F100 BL *4-31*
F100 BLR *4-31*
F100 BLS *4-31*
F100 BU *4-28*
F100 BUB *4-29*
F100 CONFIG *4-19*
F100 DHCP *4-13*
F100 EA *4-14*
F100 G *4-15*
F100 IC *4-16*
F100 IP *4-14*
F100 K I L L *4-30*
F100 L *4-26*
F100 LOCK *4-26*
F100 P *4-16*
F100 PI *4-35*
F100 PL *4-33—4-35*
F100 PLR *4-34*
F100 PLS *4-34*
F100 PN *4-32*
F100 PR *4-33*
F100 PRESETALL *4-32*
F100 PT *4-27*, *4-35*
F100 SM *4-15*
F100 ST *4-17*
F100 VER *4-18*
F18 *4-6*
F36 *4-7*
F53 *4-7*
F60 *4-8*
F67 *4-10*
F72 *4-10*
Fault Status Request (F72) *4-10*
Formats
Serial/Telnet Commands *4-1*
Frame *1-8*
Frequency *1-5*
Front Panel *1-7*, *2-8*
Display *3-9*
Power-Up Sequence *2-6—2-8*
Interface *2-8—2-9*
FTP *1-6*, *1-8*
Configuring NTP *4-21—4-25*
Configuring SNMP *4-24*
Installing and Using Software *4-19*
Function Commands *4-3*

G

Gateway (F100 G) *4-15*
Good Satellite *4-8*
GPS *1-2*, *2-3*, *2-8*, *3-3*, *A-3*
Lock Status Fault Detector (F72) *4-10*
Satellite Status Web Page *3-2*
Status Web Page *3-2*
Guest Login Password *4-36*

H

Home Page *3-2*
Host *1-6*, *A-4*
HTTP *1-2*, *1-8*, *3-1*, *3-15*
Access *3-1*
Protocol *1-6*
Humidity *1-4*
HyperTerminal
Reconnecting to Last Session *3-14*
Setting Up a Session *3-12—3-14*
Starting *3-10—3-11*

I

IEEE *1-8*
Informational Messages *5-3*
Initialization *2-6*
Installation *2-1*
Interface Specifications *1-8*
Internal Timing Performance Specifications *1-5*
Internet
Access
through Telnet *3-7—3-9*
Configuration
NTP *3-4*
SNMP *3-6*
Protocol *3-1*
IP Address *4-14*

K

Keypad *1-7*, *4-3*
Operation *2-9*

L

LCD *2-8*
Leap Indicator *A-2*
Leap Second *4-10*, *A-2*
Command (F67) *4-10*
LED *1-7*
Local Time Source Precision *A-3*
Location *1-2*, *3-1—3-2*
Lock Display Request
(F100 L) *4-26*
Login *3-7*, *4-16*, *4-33*
Serial/Telnet Interface Passwords *4-36*
Telnet, During Set-Up *3-8*
Logout *4-36*
Security *2-11—2-12*

M

Mast Mounting (Antenna) *2-3*
MD5 *D-5*
Keys *4-22—4-23*, *B-1*
Keys File Window *3-5*
NTP Broadcast Mode
with Authentication *4-22—4-23*, *B-3*
without Authentication *B-4*
Protocol *1-6*
Memory *2-2*
Checksum Test Status (F100 ST) *4-17*
Messages
Error *5-1—5-2*
Informational *5-3—5-4*
MIB *2-14*, *D-1—D-2*, *D-4*
Protocol *1-6*
MIB II *D-1*
Protocol *1-6*
MIlls, Dr. David *1-2*, *B-1*
Web Site *B-2*
Minor *5-1*
Mode *A-2*
Survey Static *4-7*
Mounting
Chassis *2-1*

N

Navigation
through Web Pages *3-3*
NET Port *1-2*, *1-7—1-8*, *2-2*, *3-7*, *3-9*, *3-15*
Configuration
Single Entry (F100) *4-11*
Default Gateway (F100 G) *4-15*
IP Address (F100 IP) *4-14*
Network Configuration
Commands (F36 or F100) *4-7*
Initial *2-13—2-14*
Using Serial/Telnet Commands *4-11*
Using the Internet *3-3*, *3-6*
Network Information Web Page *3-2*
Subnet Mask (F100 SM) *4-15*
Network Time Protocol, See NTP
Non-Standard Features *E-1*
Non-Volatile Memory *4-17*
NTP *1-6*
Broadcast Mode
Editing MD5 Keys *4-22—4-23*
with Authentication *4-22—4-23*, *B-3*
without Authentication *B-4—B-5*
Client *1-7*
Configuration *4-21*
Using FTP *4-21—4-25*
Using the Internet *3-4—3-5*
Data Packet *2-8*, *A-2*
Multicast *1-8*
Stabilization *2-7*
Synchronization Specifications *1-6*
V 3.0 Data Format (RFC-1305) *A-2*
"get" and "set" Commands *4-19*
ntp.conf file *3-4*, *4-21—4-23*
ntp.keys file *3-4*, *4-21—4-23*

O

Operating Altitude *1-4*
Operating Mode Request (F53) *4-7*
Operator *3-3*
Login Password *4-36*

P

Packet *1-6*
See also, NTP Data Packet
Parameters
Network Configuration, Initial *2-13—2-14*
Password *3-3*
Changing *4-36*
Default
Changing *3-3*
Telnet *3-8*
Default, Web Page *3-3*
Protection *2-10—2-12*
Size *4-16*
PDU *D-2*
Physical Specifications *1-3*
Position *1-1*, *2-7—2-8*, *3-1*, *5-3*

Power Specifications *1-5*
Precision *A-2—A-3*
PRN Number for Satellite *4-8*
Procomm *3-7*
Protocols, List of Supported *1-6*

R

Rack Mounting Instructions *2-1*
RAM *4-17*
    test status (F100 ST) *4-17*
Receiver *2-3*
Reference Timestamp *A-4*
Remote Configuration
    NTP *3-4*
    SNMP *3-6*
Remote Control
    Lockout (F100 LOCK) *4-26*
    Through Web Pages *3-3*
Remote Control/Configuration
    Lockout (F100 LOCK) *2-11*
RFC-1155 *1-6*
RFC-1157 *1-6*, *D-1*
RFC-1212 *1-6*
RFC-1213 *1-6*, *D-1—D-2*
RFC-1305 *1-2*, *1-6*, *A-2*, *A-4*, *B-2*
RFC-1321 *1-6*, *B-2*
RFC-1354 *D-1*
RFC-2030 *1-2*, *1-6*, *A-5*
RFC-2068 and 2616 *1-6*
RFC-2132 *1-6*
RFC-854 *1-6*
RFC-867 *1-6*, *C-2*
RFC-868 *1-2*, *1-6*, *E-1*
RFC-959 *1-6*
RG-58 *2-3*
RG-59 *1-3*, *2-3*
RJ-45 *1-2*, *1-8*, *2-2*, *2-5*
Root Delay *A-3*
RS-232 *1-8*, *2-2*, *2-5*, *3-9*
    Pinouts and Signal Levels *3-9*

S

Satellite *2-3*
    Acquisition *2-6*
    Current *4-8*
    Enabled *4-8*
    Good/Bad *4-8*
    Number Currently Tracked (F53) *4-7*
    PRN Number *4-8*
    Tracked
        List *4-8*
Security *2-10—2-12*, *3-3*, *4-36*, *D-2*
    Automatic Time Out *2-12*
Self Test Status (F100 ST) *4-17*
Serial *1-2*, *1-8*, *2-2*, *3-3*, *3-7*, *3-9*
    Access *3-9—3-14*
        Remote Control Lockout (F100 LOCK) *4-26*
    Commands
        and Responses, Common Elements *4-5*
        List *4-3—4-4*
        Semicolon used as replacement *4-2*
    Interface, Login Passwords *4-36*
Server *1-6*, *3-1*, *4-13*
    Renaming *4-22*
Session *3-7*, *3-14*, *5-3—5-4*
    Timers *3-15*
SMI *1-6*
SNMP *1-6*, *1-8*, *2-14*, *D-1—D-2*
    Configuration
        Using FTP *4-24*
        Using the Internet *3-6*
        "get" and "set" Commands *4-19*
SNTP *1-2*, *1-6*, *1-8*
    Client *1-7*
    V 3.0 Data Format (RFC-2030) *A-5*
Software Version Request
    F100 VER *4-18*
    F18 *4-6*
Specifications
    Environmental *1-4*
    Interface *1-8*
    Internal Timing Performance *1-5*
    NTP Synchronization *1-6*
    Physical *1-3*
    Power *1-5*
Status Indicators (LED) *1-7*
Status Message Window *3-3*
Storage Altitude *1-4*
Stratum *A-2—A-4*
Structure of Management Information (SMI) *1-6*
Subnet Mask (F100 SM) *4-15*
Supported Applications *1-8*
Supported Protocols *1-6*
Survey Static Mode *4-7*
Synchronization *1-2*, *1-5*, *1-7*, *2-8*

T

TCP *1-6*, *C-1—C-2*
TCP/IP *1-2*, *1-8*, *3-1*, *D-4*
Telnet *1-2*, *1-6*, *1-8*, *3-1*, *3-3*
    Commands
        and Responses, Common Elements *4-5*
        List *4-3—4-4*
        Semicolon used as replacement *4-2*
    Default Password *3-8*
    Interface, Login Passwords *4-36*
    Internet Access *3-7—3-9*
    Login, During Set-Up *3-8*
    Logout *4-36*
    Remote Control Lockout (F100 LOCK) *2-11*

Session Timer *3-7*, *3-15*
Temperature *1-4—1-5*
Terminal *2-2*, *3-9—3-10*
Terminal Strip
-48 VDC model *2-4*
Test Status (F100 ST)
RAM test *4-17*
Time and Date Entry/Request (F03) *4-6*
Time Information Web Page *3-2*
TIME Protocol *1-6*, *C-1*
Timeout *3-9*
Timers
Session *3-15*
Tracked *4-7—4-8*
Tracked Satellite *4-8*
Trap *D-2—D-4*

U

UDP *1-6*, *A-2*, *C-1—C-2*, *D-5*
User Password
Changing (F100 P) *4-16*
UTC *1-5*, *2-7*, *4-6*
Time *2-7—2-8*, *C-1—C-2*
Default Format *2-7*
Utility Port *3-7*, *3-9—3-10*, *4-3*, *5-3*
Session Timer *3-15*

W

Warranty *1-2*
Web
Access *3-1*
Browser *3-1—3-2*, *3-15*
Addresses *A-1*, *B-2*, *D-1*
Interface *1-2*, *3-1*
Leaving *3-7*
Pages *3-2*
Access to *3-2*
Configuration Control Login *3-3*
GPS Control *3-3*
Network Control *3-3*
Satellite Control *3-3*
Time Control *3-3*
Default Password *3-3*
GPS
Satellite Status *3-2*
Status *3-2*
Home *3-2*
Navigation *3-3*
Network Information *3-2*
Time Information *3-2*
Session Timer *3-15*
Windows *3-1*, *3-7*, *3-10*

Z

"get" Command - SNMP (F100 CONFIG) *4-19*
"set" Command - SNMP (F100 CONFIG) *4-19*